

(19)日本国特許庁 (J P)

(12) 公 開 特 許 公 報 (A)

(11)特許出願公開番号

特開平9-115019

(43)公開日 平成9年(1997)5月2日

(51)Int.Cl.<sup>6</sup>

G 0 7 B 15/00

識別記号

序内整理番号

F I

G 0 7 B 15/00

技術表示箇所

M

審査請求 未請求 請求項の数10 O L (全 27 頁)

(21)出願番号 特願平7-271219

(22)出願日 平成7年(1995)10月19日

(71)出願人 000004260

株式会社デンソー

愛知県刈谷市昭和町1丁目1番地

(72)発明者 前田 麻子

愛知県刈谷市昭和町1丁目1番地 日本電装株式会社内

(72)発明者 安藤 俊秀

愛知県刈谷市昭和町1丁目1番地 日本電装株式会社内

(72)発明者 吉田 一郎

愛知県刈谷市昭和町1丁目1番地 日本電装株式会社内

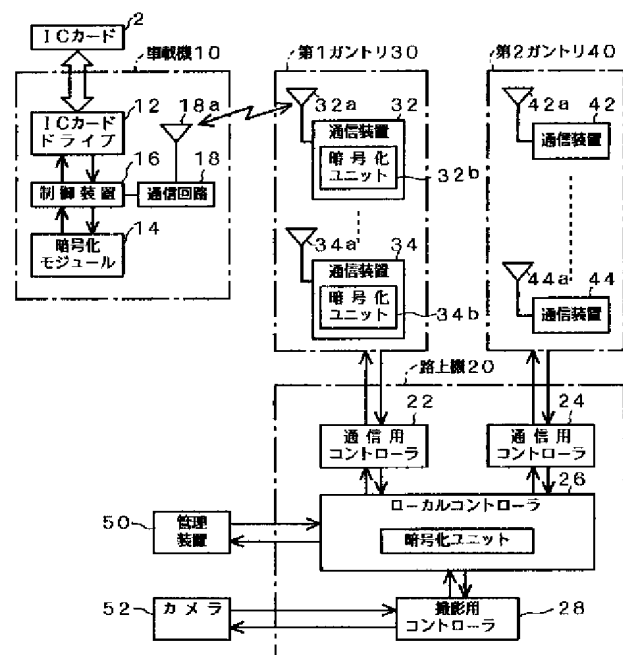
(74)代理人 弁理士 足立 勉

(54)【発明の名称】 車両用通信装置及び走行車両監視システム

(57)【要約】

【課題】 路上機との間で暗号化データを送受信する車両用通信装置において、データの暗号化を効率良く行い、通信時間を短縮する。

【解決手段】 車両走行路に設置したガントリ30、40に通信装置32、42…を設け、通信装置32、42…を介して車載機10との間で暗号化データを用いた通信を行ない、通行料金をICカード2から自動徴収するシステムにおいて、車載機10は、通信データの暗号及び復号化をガントリ30、40への侵入前及び通過後に行なう。またICカード2へのデータの書き込み等も暗号化データを用いるが、通信データの暗号化には、ICカード2とは異なり、且つ高速処理可能なアルゴリズムを用いる。この結果、通信時には路上機20側でのみデータの暗号化・復号化を行えばよく、またこれを高速に行なうことができるので、通信時間を短縮して、走行中の限られた時間内にて正確なデータ通信を実行できる。



**【特許請求の範囲】**

【請求項1】 車両の走行路付近に設置された路上機の通信エリアに入ると、路上機からの送信信号にตอบสนองして、路上機との間で所定データを暗号化した暗号化データを送受信する車両用通信装置において、送信すべきデータの暗号化を前記通信エリアへの侵入前に行ない、受信した暗号化データの復号化を路上機とのデータ通信完了後に行うように構成してなることを特徴とする車両用通信装置。

【請求項2】 所定データが格納されたICカードを着脱自在に装着可能で、該装着されたICカードに対するデータの読み出し及び書き込みを行うドライブ手段と、該ドライブ手段にICカードが装着されると、前記ドライブ手段を介してICカードから前記路上機に送信すべきデータを読み出し、該データを含む車両側データを暗号化して、該暗号化データを前記路上機への送信データとして記憶する暗号化手段と、車両が前記路上機の通信エリアに入って前記路上機からの送信信号を受信すると、前記路上機との間のデータ通信を開始し、前記暗号化手段にて暗号化され記憶された送信データを路上機側に送信すると共に、路上機側から送信されてきた暗号化データを受信して記憶する通信手段と、該通信手段が前記路上機とのデータ通信を完了すると、前記通信手段にて受信され記憶された路上機側からの暗号化データを復号化すると共に、該復号化した受信データに基づき前記ドライブ手段を介してICカードに通信結果を書き込む復号化手段と、を備えたことを特徴とする請求項1記載の車両用通信装置。

【請求項3】 前記復号化手段は、前記ICカードへの通信結果の書き込みを、前記暗号化手段及び復号化手段において送信データの暗号化及び受信データの復号化に使用される通信用暗号化アルゴリズムとは異なるカード用暗号化アルゴリズムにて暗号化した暗号化データにて行うことを特徴とする請求項2記載の車両用通信装置。

【請求項4】 前記ドライブ手段にICカードが装着されると、前記暗号化手段が前記送信データを生成する前に、所定の認証用データを用いてICカードと当該装置との間で互いに正常な装置であるかを確認する相互認証を実行させ、該認証結果を路上機に送信すべきデータの一つとして、前記暗号化手段に送信データを生成させる認証手段を備え、しかも該認証手段は、前記ICカードとの間でやり取りする認証用データとして、前記カード用暗号化アルゴリズムにて暗号化した暗号化データを用いること特徴とする請求項3記載の車両用通信装置。

【請求項5】 前記通信用暗号化アルゴリズムは、前記カード用暗号化アルゴリズムに比べてデータを高速に暗号化可能な暗号化アルゴリズムであることを特徴とする

請求項3又は請求項4記載の車両用通信装置。

【請求項6】 請求項1～請求項5いずれか記載の車両用通信装置において、更に、当該装置の動作或は送信すべきデータの異常を判定する異常判定手段を備え、該異常判定手段にて異常が判断されると、前記送信データにその旨を表わすエラーデータを付与し、路上機とのデータ通信により当該装置側の異常を路上機側に報知するよう構成してなることを特徴とする車両用通信装置。

【請求項7】 請求項1～請求項6いずれか記載の車両用通信装置からなる車載機と、該車載機を搭載した車両が走行可能な走行路付近に設置された路上機とにより構成され、該路上機側にて、車載機との間で暗号化データを用いたデータ通信を行うことにより、該路上機の通信エリアに侵入した車両又は車両乗員を特定して所定の処理を行う走行車両監視システムであって、車載機及び路上機において夫々送信すべきデータを暗号化する暗号化手段は、該データの一部を暗号化し、送信データとして、暗号文と暗号化されていない平文とが混在した暗号化データを生成することを特徴とする走行車両監視システム。

【請求項8】 請求項1～請求項6いずれか記載の車両用通信装置からなる車載機と、該車載機を搭載した車両が走行可能な走行路付近に設置された路上機とにより構成され、該路上機側にて、車載機との間で暗号化データを用いたデータ通信を行うことにより、該路上機の通信エリアに侵入した車両又は車両乗員を特定して所定の処理を行う走行車両監視システムであって、路上機において車載機との間でデータ通信を行う路上機側通信手段は、当該路上機の通信エリア内に前記車載機を搭載した車両がない通常時には、車載機起動用のパイロット信号を周期的に送信し、該パイロット信号送信時に該パイロット信号を受信した車載機側から応答信号が送信され、該応答信号を受信すると、前記パイロット信号の送信を停止して、該応答信号を送信してきた車載機との間でデータ通信を行い、該データ通信が完了すると、その旨を表わす通信完了信号を送信して、前記パイロット信号の送信を再開するよう構成され、車載機において路上機との間でデータ通信を行う車載機側通信手段は、前記パイロット信号を受信すると前記路上機に応答信号を送信して、前記路上機との間のデータ通信を開始し、該データ通信の完了後は、前記通信完了信号を受信してデータ通信の完了を確認するように構成され、しかも、前記路上機側通信手段は、車載機とのデータ通信完了時に、前記通信完了信号に続けて前記パイロット信号を送信することを特徴とする走行車両監視システム。

【請求項9】 前記路上機側通信手段は、パイロット信号又は送信データを送信した後、所定期間、無変調の搬送波を送信し、前記車載機側通信手段は、前記路上機側

から送信されてくる搬送波を前記応答信号又は送信データに応じて変調することにより、路上機側に応答信号及び送信データを送信するよう構成され、

しかも、前記車載機側通信手段は、前記データ通信の完了後、前記路上機側からの通信完了信号を受信できないときには、前記路上機側通信手段からの搬送波を利用して、前記路上機側に通信完了信号の要求信号を送信することを特徴とする請求項8記載の走行車両監視システム。

【請求項10】 請求項7～請求項9いずれか記載の走行車両監視システムにおいて、

前記路上機は、有料道路の入り口又は出口に配設され、前記車載機とのデータ通信により車載機側から送信されてくる通行料金の支払情報を表わす暗号化データを復号化し、該支払情報に従い通行料金を徴収すると共に、該料金徴収結果を暗号化して車載機側に送信する料金徴収用路上機であり、

前記車載機は、前記路上機とのデータ通信により前記支払情報を暗号化して前記路上機に送信し、その後前記路上機から送信されてくる前記料金徴収結果を表わす暗号化データを復号化して記憶する通行料金支払用車載機であり、

しかも、前記車載機－路上機間でのデータ通信に使用されるデータ構成を、前記通行料金の徴収形態にかかわらず全て共通にしてなることを特徴とする走行車両監視システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、車両の走行路付近に配置された路上機との間で暗号化データを用いたデータ通信を行う車両用通信装置、及び該装置と路上機とにより構成されて路上機付近を走行する車両を監視する走行車両監視システムに関し、特に有料道路を走行する車両から通行料金を自動徴収するのに好適な装置に関する。

【0002】

【従来の技術】従来より、有料道路において通行料金を走行中の車両から自動徴収する課金システムが知られている。この課金システムは、有料道路の入り口や出口に通信装置（路上機）を設置すると共に、有料道路を通行する車両に、路上機からの問い合わせに回答して乗員固有のデータや料金の支払方法を表わすデータ等を送信する通信装置（車載機）を設けて、路上機側で車載機からの送信データに基づき通行料金を自動徴収するものである。

【0003】ところで、こうしたシステムでは、車載機と路上機との間で、料金データ、車両データ、乗員データ等のプライベートな情報が無線通信されるため、そのデータが第三者に傍受されて悪用される虞がある。例えば料金の支払にキャッシュカードを用いるような場合に

は、そのカードの情報が読み取られて、不正に使用される虞がある。

【0004】そこで、こうした問題を解決するために、従来では、例えば特開平6-60237号公報に開示されているように、車載機と路上機との間のデータ通信を、送信すべきデータを暗号化した暗号化データを用いて行うことにより、第三者に傍受されても、そのデータ内容が容易に読み取られないようにすることが提案されている。

【0005】

【発明が解決しようとする課題】ところで、上記提案のシステムでは、送信データを暗号化するのに、ICカード等に情報の読み書きを行うのに規格化された周知のデータ暗号化標準（DES）アルゴリズムが使用されるため、車載機－路上機間の通信データが傍受されて解析されると、比較的容易に復号化され、機密性が悪いといった問題があった。また、こうしたDESアルゴリズムは、データの暗号化に時間がかかり、暗号化の高速度化を図り難いアルゴリズムであるため、車載機が路上機の通信エリア内に侵入してから、車載機及び路上機において、送信データの暗号化及び受信データの復号化を行うようにしていると、その暗号化及び復号化に時間がかかり、車両の速度が高い場合に、データ通信が完了していない状態で車載機が路上機の通信エリアを脱出してしまうといった問題もあった。

【0006】例えば、上記のような課金システムにおいて、車載機がキャッシュカード等への情報書込（料金徴収）行い、完了後にその情報を暗号化して路上機に送信する場合、車載機は、まず、料金徴収のために路上機から送信されてきたデータを復号化し、次にこの復号化したデータに従いキャッシュカード等へ情報を書き込み、その後、書き込んだ結果を暗号化して、路上機側に送信することになるが、車載機が路上機からのデータの復号化と路上機に送信すべきデータの暗号化を行うためには時間を要する。つまり、例えば、暗号化及び復号化に要する時間を夫々30msec.とし、車両の走行速度が120km/hとすると、車載機が暗号化又は復号化を1回行うたびに車両は1m走行することになる。一方、路上機の通信エリアは、複数の車両が同時に侵入しないように、通常、車両の大きさ程度に設定されることから、通信エリア内での車両の走行距離は数m程度である。従って、車両が120km/h程度で走行する高速道路において、路上機と車載機とのデータ通信を正常に行うようにするには、一方向の通信だけでも車載機側及び路上機側での暗号化及び復号化処理が必要であるため、路上機と車載機との間のデータ通信回数（往復通信）は1～2回が限界であり、通信回数をそれ以上多くすると、車載機は通信エリアを脱出してしまい、正常なデータ通信を行うことができなくなる。

【0007】一方、こうした問題を解決するには、車両

の走行速度を制限するとか、DESアルゴリズムに従って暗号化を行う暗号化装置を、高速処理可能な装置に変更すればよいが、車両の走行速度を制限すると、路上機付近で交通渋滞が発生するようになって、無線通信にて通行料金の自動徴収することにより得られる交通渋滞の低減効果を充分発揮できなくなり、逆に暗号化装置を高速にするには、高価な暗号化装置を用いる必要があり、路上機側では対応できても、車載機に高価な暗号化装置を搭載するには、使用者個人の負担が大きくなるため、実現は難しい。

【0008】また、暗号化アルゴリズムを、DESアルゴリズム以外のもの、例えば電子回路等のハード構成によるパイプライン処理にて暗号化が可能な暗号化アルゴリズム、に変更することにより、暗号化を高速に行うようにすることも考えられるが、この場合にも、暗号化装置を、CPUを用いたソフト処理ではなく、専用のハード構成によるパイプライン処理にて暗号化を行うように構成するには、暗号化装置自体が高価になるため、路上機側では対応できても、車載機側にこうした暗号化装置を設けることは困難である。

【0009】本発明は、こうした問題に鑑みなされたもので、送信すべきデータの暗号化を効率良く行い、狭い通信エリア内での通信を短時間で行うことができ、しかも、通信データの傍受等により生じる不正を良好に防止できる車両用通信装置、及びこの車両用通信装置を用いた前記課金システム等の走行車両監視システムを提供することを目的とする。

【0010】

【課題を解決するための手段】かかる目的を達成するためになされた請求項1に記載の車両用通信装置においては、車両の走行路付近に設置された路上機の通信エリアに入ると、路上機からの送信信号にตอบสนองして、路上機との間で所定データを暗号化した暗号化データを送受信する。そして、こうしたデータ通信に用いる送信すべきデータの暗号化は、路上機の通信エリアへの侵入前に行ない、受信した暗号化データの復号化は、路上機とのデータ通信が完了してから行う。

【0011】即ち、送信データの暗号化及び受信データの復号化には時間がかかるので、本発明では、こうしたデータの暗号化及び復号化を、路上機との通信を行わない領域内で（換言すれば当該通信装置側での処理に余裕のある期間内に）行うのである。

【0012】このため、本発明の車両用通信装置によれば、当該車両用通信装置が路上機との間でデータ通信を行う際の通信時間を短縮でき、前述のように、車両の走行速度を制限したり、データの暗号化及び復号化を行う暗号化装置に高価なものを使用することなく、路上機との間のデータ通信を正確に行うことができる。

【0013】次に、請求項2に記載の車両用通信装置においては、路上機に送信すべき所定データが格納された

ICカードを着脱自在に装着可能で、その装着されたICカードに対するデータの読み出し及び書き込みを行うドライブ手段が備えられ、ドライブ手段にICカードが装着されると、暗号化手段が、このドライブ手段を介してICカードから路上機に送信すべきデータを読み出し、その読み出したデータを含む車両側データを暗号化して、その暗号化データを路上機への送信データとして記憶する。

【0014】そして、車両が路上機の通信エリアに入ると路上機からの送信信号を受信すると、通信手段が、路上機との間のデータ通信を開始し、暗号化手段にて暗号化され記憶された送信データを路上機側に送信すると共に、路上機側から送信されてきた暗号化データを受信して記憶する。

【0015】そしてその後、通信手段が路上機とのデータ通信を完了し、当該通信装置の負荷が軽くなると、復号化手段が、通信手段にて受信され記憶された路上機側からの暗号化データを復号化すると共に、その復号化した受信データに基づきドライブ手段を介してICカードに通信結果を書き込む。

【0016】即ち、本発明の車両用通信装置においては、路上機に送信すべきデータの少なくとも一部（例えば運転者の識別コードや銀行口座等を表すプライベート情報等）や路上機との通信結果を記憶するのにICカードが使用されるが、このICカードからのデータの読み出し及び路上機に送信すべき車両側データの暗号化を、ICカードがドライブ手段に装着されたときに行い、また路上機から送信され受信したデータの復号化及び復号化したデータから得られる通信結果のICカードへの書き込みを、路上機との間のデータ通信を完了してから行うことにより、車両が路上機とのデータ通信を行う際には、データの暗号化及び復号化を実行しないようにしている。

【0017】このため、本発明の車両用通信装置においても、請求項1に記載の装置と同様、当該車両用通信装置が路上機との間でデータ通信を行う際の通信時間を短縮でき、車両の走行速度を制限したり、データの暗号化及び復号化を行う暗号化装置に高価なものを使用することなく、路上機との間のデータ通信を正確に行うことができる。

【0018】また、ICカードに対するデータの読み書きには、通常、データをシリアル伝送するようにされており、ドライブ手段によるICカードへのアクセス時間が長くなるが、本発明の車両用通信装置では、こうしたICカードに対するデータの読み書きも、路上機との間のデータ通信を行っていないタイミングに行われるため、ICカードに対するデータの読み書きによって通信時間が長くなることもなく、路上機との通信時間を短縮できる。

【0019】なお、前述した課金システムのように、通

信結果（料金徴収に関する情報）をICカードに書き込み、その結果を、再度路上機側に知らせる必要がある場合には、ICカードに通信結果を書き込んだ後、車両が次に路上機の通信エリアに侵入するまでの間に、その結果を送信データとして暗号化しておき、車両が次に路上機の通信エリアに入ったときに、その暗号化データを路上機に送信するようにすればよい。

【0020】また次に、請求項3に記載の車両用通信装置においては、復号化手段がICカードへのデータの書き込みを行う際には、暗号化手段及び復号化手段において送信データの暗号化及び受信データの復号化に使用される通信用暗号化アルゴリズムとは異なるカード用暗号化アルゴリズムにて暗号化した暗号化データを用いて行う。

【0021】つまり、従来より、ICカードへのデータの書き込みを行う際には、カードデータの不正な変更等を防止するために、通常、前述のDESアルゴリズム等を用いた暗号化データを用いて行うようにされているが、この場合、ICカードへのデータの書き込みを行う際の暗号化アルゴリズムと、路上機との通信に用いる暗号化アルゴリズムとを同じにすると、路上機との間の通信信号を復号化し易くなる。そこで、本発明では、カード用暗号化アルゴリズムと通信用暗号化アルゴリズムとを異なるアルゴリズムにすることにより、通信信号が傍受されても送受信データ、特にICカードから読み出したプライベート情報を復号化し難くし、通信の機密性を向上しているのである。

【0022】このため、本発明の車両用通信装置によれば、ICカードから読み出され、路上機に送信される、銀行口座やパスワード等のプライベート情報が、不正に傍受・解読されて、ICカードが偽造されるのを未然に防止し、こうした犯罪の発生を抑制できる。

【0023】また、請求項4に記載の車両用通信装置においては、ドライブ手段にICカードが装着されると、認証手段が、暗号化手段が送信データを生成する前に、所定の認証用データを用いてICカードと当該装置との間で互いに正常な装置であるかを確認する相互認証を実行させ、その認証結果を路上機に送信すべきデータの一つとして暗号化手段に送信データを生成させる。そして、認証手段は、ICカードとの間でやり取りする認証用データとして、カード用暗号化アルゴリズムにて暗号化した暗号化データを用いる。

【0024】つまり、前述の課金システム等においては、ICカードは勿論のこと、車両用通信装置自体を偽造して、路上機に対して料金を支払ったように見せ掛ける不正が行われる虞がある。そこで、本発明では、車両用通信装置とICカードとの間でカード用暗号化アルゴリズムを用いた暗号化データにて相互認証させ、その認証結果が正常であれば、その認証結果を路上機に送信すべきデータの一つとして、暗号化手段による送信データ

の暗号化を実行させることにより、路上機側にて、受信データが正規の車両用通信装置からの送信データかどうかを判別できるようにしている。

【0025】従って、本発明の車両用通信装置によれば、偽造した通信装置を用いた不正なデータ通信を排除して、路上機との間のデータ通信の安全性を高めることができる。なお、路上機との間のデータ通信を偽造した通信装置を用いて不正に行う方法として、正規の車両用通信装置からの送信信号自体をコピーして、それを送信することも考えられるが、こうした不正に対しては、車両用通信装置と路上機との間でデータを暗号化するのに使用される通信用の暗号鍵を定期的或は不定期に変更することにより対応できるため、車両用通信装置としても、暗号鍵を路上機との間でやり取りして、頻繁に切り換えるようにすることが望ましい。

【0026】次に、請求項5に記載の車両用通信装置においては、通信用暗号化アルゴリズムとして、カード用暗号化アルゴリズムに比べてデータを高速に暗号化可能な暗号化アルゴリズムが使用される。これは、本発明の車両用通信装置では、路上機側に送信すべきデータの暗号化を、路上機とのデータ通信を行わない領域で実行するため、当該通信装置側で要する通信時間は短縮できるものの、路上機側では、当該通信装置とデータ通信を行っている最中に、受信データの復号化及び送信データの暗号化を行う必要があるためである。

【0027】つまり、本発明では、通信用暗号化アルゴリズムを、カード用暗号化アルゴリズム（一般に前述のDESアルゴリズムが使用される）よりも高速な暗号化アルゴリズムを使用することにより、路上機側でデータの暗号化及び復号化に要する時間を短縮して、路上機との間の通信時間をより短縮できるようにしているのである。従って、本発明によれば、高速走行中の車両と路上機との間のデータ通信をより確実に行うことができるようになる。

【0028】また、請求項6に記載の車両用通信装置においては、当該装置の動作或は送信すべきデータの異常を判定する異常判定手段を備え、この異常判定手段にて異常が判断されると、送信データにその旨を表わすエラーデータを付与することにより、その後実行される路上機との間のデータ通信によって、当該装置側の異常を路上機側に報知できるように構成される。

【0029】この結果、路上機側では、通信エリア内に入った車両に搭載された車両用通信装置の異常を検知でき、その検知結果から、例えば、車両運転者に対して車両を停止させよとのメッセージを音声、表示等により送るとか、走行中の車両をカメラで撮影して路上機の管理者に知らせる、といった対策を自動で行うことができるようになる。

【0030】一方、請求項7～請求項10に記載の走行車両監視システムは、上述した請求項1～請求項6いず

れか記載の車両用通信装置からなる車載機と、この車載機を搭載した車両が走行可能な走行路付近に設置された路上機とにより構成され、路上機側にて、車載機との間で暗号化データを用いたデータ通信を行うことにより、該路上機の通信エリアに侵入した車両又は車両乗員を特定して、例えば、有料道路の通行料金、駐車場の駐車料金、各種施設への入場料金等の自動聴取を行うとか、所定施設に入場しようとする車両や乗員を監視して不審者の侵入を防止する、といった所定の処理を行うものである。

【0031】そして、請求項7に記載の走行車両監視システムにおいては、車載機及び路上機において夫々送信すべきデータを暗号化する暗号化手段が、データの一部を暗号化することにより、送信データとして、暗号文と暗号化されていない明文とが混在した暗号化データを生成するように構成される。

【0032】つまり、車載機と路上機との間のデータ通信において、通信信号が傍受されてデータが解読されないようにするには、既述したようにデータを暗号化するのに使用される暗号鍵を定期的或は不定期に変更するようにするとよいが、この場合、暗号化データを受信した装置側で使用した暗号鍵が分かるように、暗号鍵を表わすデータを送信する必要がある、このデータから暗号鍵が解読されると、データ自体も解読されることになる。

【0033】そこで、本発明では、こうした対策とは別に、プライベートデータ等を暗号化するに当たって、そのデータの全文を暗号化するのではなく、データの一部を暗号化して、送信データを、暗号文と明文とが混在した暗号化データとすることにより、このデータをより解読し難くしているのである。

【0034】このため、本発明の走行車両監視システムにおいては、車載機—路上機間にて送受信される通信データが第三者に解読されるのをより確実に防止して、システムの信頼性を向上することができ、また、通信データの不正使用による犯罪の発生を抑制できる。

【0035】また、請求項8に記載の走行車両監視システムにおいては、通常、路上機側通信手段が、自己の通信エリア内に車載機起動用のパイロット信号を周期的に送信しており、この通信エリア内に車両が侵入して、その車両に搭載された車載機側通信手段がパイロット信号を受信すると、車載機側通信手段が、路上機に対して応答信号を送信する。すると、路上機側通信手段は、この応答信号を受信して、パイロット信号の送信を停止し、その後、応答信号を送信してきた車載機との間でデータ通信を行う。また、このデータ通信が完了すると、路上機側通信手段が、その旨を表わす通信完了信号を車載機側に送信し、車載機側通信手段は、この通信完了信号を受信することによりデータ通信の完了を確認する。

【0036】即ち、本発明の走行車両監視システムにおいては、路上機から送信されるパイロット信号により車

載機が起動してデータ通信を開始し、その後は、路上機側では通信完了信号を送信することによりデータ通信を終了し、車載機側ではこの通信完了信号を受信することによりデータ通信を終了する。

【0037】ところで、路上機側では、通信完了信号を送信してデータ通信を終了すると、パイロット信号の周期的な送信に移行することになるのであるが、通信完了信号送信後に一定時間間隔でパイロット信号を送信するようにすると、データ通信終了時に既に次の車両が通信エリア内に侵入していたとしても、この車両の車載機を起動できるのは、通信完了信号送信後、次にパイロット信号の送信タイミングになったときであり、その車載機とのデータ通信の開始が遅れてしまう。

【0038】そこで、本発明では、路上機側通信手段を、車載機とのデータ通信完了時に通信完了信号を送信する際には、この信号に続けてパイロット信号を送信するように構成している。この結果、本発明によれば、路上機の通信エリア内に複数の車両が連続的に侵入してくるような場合に、ある車載機との通信完了後に、次の車載機を速やかに起動させて、その車載機とのデータ通信を速やかに開始することができるようになる。従って、車載機の起動が遅れて、その車載機との通信可能時間が短くなり、正常なデータ通信が実行できなくなる、といったことを防止できる。

【0039】また次に、請求項9に記載の走行車両監視システムにおいては、路上機側通信手段が、パイロット信号又は送信データを送信した後、所定期間、無変調の搬送波を送信し、車載機側通信手段が、路上機側から送信されてくる搬送波を応答信号又は送信データに応じて変調することにより、路上機側に応答信号及び送信データを送信する。そして、車載機側通信手段は、路上機との間のデータ通信完了後に、路上機側からの通信完了信号を受信できないときには、路上機側通信手段からの搬送波を利用して、路上機側に通信完了信号の要求信号を送信する。

【0040】つまり、本発明の走行車両監視システムにおいては、路上機がデータ通信の主導権をもち、車載機は、路上機からの送信信号に応答してデータを送信するようにされており、データ通信完了後、車載機は、路上機側から送信されてくる通信完了信号を受信することにより、データ通信の終了を確認するのであるが、車載機がノイズ等の何等かの原因で路上機からの通信完了信号を受信できなかった場合には、車載機側でデータ通信を正常に行えたかどうかを判別できないため、通信エラーとして処理するしかない。しかし、この場合、路上機側では、データ通信を正常に実行できたとして、通信完了信号を送信しているので、車載機側と路上機側とでデータ処理が異なってしまう。

【0041】そこで本発明では、一連のデータ通信が終了した後、車載機側にて路上機からの通信完了信号を受

信できない場合には、路上機が周期的に送信してくる搬送波を利用して、路上機側に通信完了信号の要求信号を送ることにより、路上機に通信完了信号を受信できていないことを知らせるようにしているのである。

【0042】この結果、本発明によれば、データ通信完了後に車載機が路上機からの通信完了信号を受信できなかった場合でも、車両が路上機の通信エリア内にいる間は、路上機から通信完了信号を再送信させて、路上機と車載機とが共にデータ通信が正常に完了したことを確認できるようになり、データ通信の精度を向上できる。

【0043】次に、請求項10に記載の走行車両監視システムにおいては、路上機が、有料道路の入り口又は出口に配設され、車載機とのデータ通信により車載機側から送信されてくる通行料金の支払情報を表わす暗号化データを復号化し、その支払情報に従い通行料金を徴収すると共に、料金徴収結果を暗号化して車載機側に送信し、車載機が、路上機とのデータ通信により支払情報を暗号化して路上機に送信し、その後路上機から送信されてくる料金徴収結果を表わす暗号化データを復号化して記憶する。つまり、本発明の走行車両監視システムは、有料道路を走行する車両に対する通行料金の徴収を車載機と路上機とのデータ通信により自動で行う有料道路の課金システムである。

【0044】ところで、有料道路には、料金一律の有料道路もあれば、走行距離或は道路の利用時間によって料金が設定される料金変動型の有料道路もあり、こうした料金の設定方法が異なる有料道路では、車載機と路上機とで送受信するデータ内容も異なることになる。また、通行料金の支払方法も、キャッシュカードを用いた場合のように、指定した銀行口座から料金を引き出させる方法とか、プリペイドカードのように予め任意の料金を支払っておき、その中から徴収させて残高を更新する方法等、種々の方法が考えられ、このように支払方法が異なる場合にも、車載機と路上機とで送受信するデータ内容が異なることになる。

【0045】そして、このように通行料金の徴収形態（設定方法、支払方法等）が異なる場合に、各徴収形態毎に通信データのデータ構成を設定していると、車載機及び路上機において送信データを生成して暗号化したり、受信データを復号化して必要な情報を取り出す際のデータ処理が煩雑になり、車載機と路上機との通信に時間がかかるようになるとか、或は、料金の徴収形態が異なる有料道路課金システムにおいて車載機を共用できなくなるといったことが考えられる。

【0046】そこで本発明では、更に、車載機一路上機間でのデータ通信に使用されるデータ構成を、通行料金の徴収形態にかかわらず全て共通にしている。この結果、本発明によれば、車載機及び路上機における通信データの生成、暗号化及び復号化を、効率良く行うことができるようになり、データ通信に要する時間を短縮し

て、車載機と路上機との間のデータ通信を車載機が路上機の通信エリア内にいる間に正確に実行できるようにすることができる。また、通行料金の徴収形態の異なる有料道路課金システムにおいて、同じ車載機を共用させることができ、各システム毎に専用の車載機を用いる必要がないので、車両所有者の負担を軽減して、有料道路課金システムを容易に実現できるようになる。

【0047】なお、このように車載機一路上機間でのデータ通信に使用されるデータ構成を料金の徴収形態にかかわらず共通にすれば、有料道路課金システム以外のシステム、例えば駐車料金を自動徴収する課金システム等においても、通信データを構成する特定のデータの内容を変更するだけで、同じ車載機を利用できるようになり、有料道路課金システムにおいて使用される車載機を、より広汎に利用でき、車載機の稼働率を高めることができる。

【0048】

【発明の実施の形態】以下、本発明が適用された有料道路課金システムの一例を図面を用いて説明する。まず図1は、本実施例の有料道路課金システムの全体構成を表わすブロック図である。

【0049】図1に示す如く、本実施例の有料道路課金システムは、車両に搭載された車載機10と、有料道路の入り口又は出口付近に設置された路上機20とから構成される。路上機20は、複数車線からなる車両の走行路上方に、車両の進行方向に沿って所定間隔で架け渡された2つの高架台である第1ガントリ30及び第2ガントリ40を備える。そして、第1ガントリ30及び第2ガントリ40には、夫々、車両走行路上の各車線を走行する車両に搭載された車載機10との間でデータ通信を行うための通信装置32、34…及び42、44…が備えられている。

【0050】車載機10は、車両が上記各ガントリ30、40を通過する際、走行中の車線を通信エリアとする一つの通信装置、例えば通信装置32、42との間で、通行料金を支払うためのデータ通信を自動で行うためのものであり、通行料金支払のためのキャッシュカードやプリペイドカード等からなるICカード2を着脱自在に装着可能で、装着されたICカード2に対して情報の読み書きを行うドライブ手段としてのICカードドライブ12と、各ガントリ30、40に設けられた通信装置32、34…、42、44…との間で無線通信を行うための、アンテナ18aを備えた通信回路18と、送信データの暗号化及び受信データの復号化を行うための暗号化モジュール14と、これら各部を制御するマイクロコンピュータからなる制御装置16とから構成される。

【0051】なお、暗号化モジュール14は、車載機10に内蔵してもよいし外付けでもよいが、暗号化アルゴリズムや暗号化に使用する鍵データについては変更できる機能を有する。つまり暗号化モジュール14は、車載

機10から取り外して暗号化のためのソフトウェアを再プログラミングしたり、或は車載機10に固定したまま暗号化用のデータやソフトウェアを書き換えることによって、暗号化アルゴリズムや鍵データを変更できるようにされている。

【0052】第1ガントリ30に備えられた通信装置32, 34…は、車載機10との間で無線通信を行うためのアンテナ32a, 34a…を備えると共に、送信データの暗号化及び受信データの復号化を行うための暗号化ユニット32b, 34b…を備え、車載機10との間でデータ通信を行いながらデータの暗号化及び復号化を行う。これに対して、第2ガントリ40に備えられた通信装置42, 44…は、こうした暗号化ユニットを備えておらず、アンテナ42a, 44a…を介して車載機10との間でデータ通信を行うだけである。つまり通信装置42, 44…は、送信データや受信データをそのまま路上機20に入出力する。なお、図示しないが、これら各通信装置32, 34…、42, 44…は、車載機10と同様、送受信用の通信回路と、マイクロコンピュータからなる制御装置とを備え、この制御装置による制御動作の下に、車載機10との間の無線通信及び路上機20との間のデータ伝送が行われる。

【0053】次に、路上機20は、上記各ガントリ30, 40毎に設けられ、各通信装置32, 34…、42, 44…の通信動作を制御する通信用コントローラ22, 24と、これら各通信用コントローラ22, 24を介して、各ガントリ34, 40の通信装置32, 34…、42, 44…との間でデータをやり取りして、走行中の車両から通行料金を徴収するための制御を行う、コンピュータからなるローカルコントローラ26とを備える。

【0054】また路上機20には、走行中の車両を撮影するために走行路付近に設置された複数のカメラ52が接続されており、ローカルコントローラ26は、走行中の車両から通行料金を徴収できなかった場合等には、撮影用コントローラ28を介してカメラ52を駆動し、その車両を撮影する。またローカルコントローラ26は、有料道路の料金徴収を集中管理する管理装置（ホストコンピュータ）50に接続され、通行料金の徴収結果や、通行料金を正常に徴収できなかった車両情報等を管理装置50に転送する。

【0055】本実施例の有料道路課金システムにおいては、通常は、路上機20側の各通信装置32, 34, …、42, 44, …が、所定時間（ $t$  [msec.]）間隔で、対応する車線を走行中の車両に搭載された車載機10を起動するためのパイロット信号を送信し、そのパイロット信号を受信した車載機10が応答信号を送信して、その応答信号を受信できた場合に、車載機10との間で料金徴収のためのデータ通信を実行する。

【0056】一方、車載機10は、路上機20側からの

パイロット信号を受けるまでは消費電力の低減等のためにスリープ状態となり、パイロット信号を受信すると起動して、応答信号を送信し、その後、路上機20側通信装置との間で料金支払のためのデータ通信を実行する。

【0057】またこのように路上機20と車載機10との間で行われるデータ通信は、全て、路上機20の管理の下に実行される。つまり、本実施例では、路上機20側の各通信装置32, 34, …、42, 44, …は、例えば図3に示す如く、所定の送信期間 $T1$ 中に、上記パイロット信号やデータ通信のための変調信号を送信し、その後、所定の応答期間 $T2$ の間、無変調の搬送波を送信するようにされており、車載機10側では、この搬送波を変調することにより、パイロット信号に対する応答信号やデータを送信する。そして、このために、車載機10側の通信回路18は、例えば図2に示す如く構成される。

【0058】即ち、図2に示す如く、通信回路18において、アンテナ18aは、伝送路62を介してダイオード63のアノードに接続されており、ダイオード63のカソードは伝送路64を介して発振器65に接続されている。この伝送路64の長さは、路上機20側より送信されてくる搬送波の線路波長 $\lambda$ に対して $\lambda/4$ に設定されている。ダイオード63のアノード、カソードは、夫々、コイル68と抵抗器69、コイル70と抵抗器71を介して接地されている。

【0059】また、コイル68は抵抗器69に並列接続されたコンデンサ72と共にローパスフィルタを構成し、コイル70は抵抗器71に並列接続されたコンデンサ73と共にローパスフィルタを構成し、更にこれら各部は、ダイオード63と共に受信信号の包絡線検波回路80を構成している。

【0060】そして、ダイオード63のアノードは、抵抗器74及びトランジスタ $Tr3$ を介して電源 $VDD$ に接続され、発振器65は、トランジスタ $Tr1$ を介して電源 $VDD$ に接続され、コイル70と抵抗器71との接続点は、トランジスタ $Tr2$ を介して電源 $VDD$ に接続されており、これら各トランジスタ $Tr1$ ,  $Tr2$ ,  $Tr3$ のベースは、夫々、制御装置16に接続されている。

【0061】このため、通信回路18においては、制御装置16により各トランジスタ $Tr1$ ,  $Tr2$ ,  $Tr3$ がオフされている場合には、アンテナ18aにて受信された路上機20側からの送信信号が包絡線検波回路80にて包絡線検波されることになり、その検波後の信号 $S1$ は、受信データとして制御装置16に入力される。つまり、この状態では、路上機20側から図3に示す送信期間 $T1$ 内に送信されたきた変調信号を受信し、それを包絡線検波して得られる信号（2値信号となる） $S1$ を、受信データとして、制御装置16に入力できる。

【0062】次に、トランジスタ $Tr1$ ,  $Tr3$ をオフ

し、トランジスタTr 2のみをオンすると、ダイオード63のカソードに電源電圧が印加されるため、ダイオード63は抵抗器69を介して逆方向にバイアスされる。従って、この場合には、ダイオード63は受信信号の非通過状態となり、アンテナ18aからの受信信号はダイオード63の入力端子(アノード側)で反射される。一方、トランジスタTr 1, Tr 2をオフし、トランジスタTr 3のみをオンすると、ダイオード63のアノードに電源電圧が印加されるため、ダイオード63は抵抗器74, 71を介して順方向にバイアスされる。従って、この場合には、ダイオード63は受信信号を双方向に通過可能な状態となり、アンテナ18aからの受信信号は、ダイオード63を通過し、伝送路64を伝搬して、入力インピーダンスが無限大となっている発振器65の入力端子で反射し、更にこの反射波は、ダイオード63を逆方向に通過して、伝送路62を伝搬してアンテナ18aから放射される。そして、この時、伝送路64の実効線路長は $\lambda/4$ であるので、アンテナ18aから放射される信号は、トランジスタTr 1, Tr 3をオフし、トランジスタTr 2のみをオンした場合の信号に対して、位相差が $\pi$ (180度)となる。

【0063】このため、通信回路18においては、路上機20側から無変調の搬送波が送信されてくる図3に示す送信期間T 2内に、トランジスタTr 2とトランジスタTr 3とを交互にオン・オフすれば、搬送波を位相変調(PSK)して、アンテナ18aから送信できるようになる。

【0064】つまり、本実施例では、図3に示す期間T 1内に路上機20側からの送信信号を受信して検波信号S1を制御装置16に入力すると、制御装置16は、その信号に応答して送信すべきデータに応じて、トランジスタTr 2及びTr 3をオン・オフすることにより、搬送波を位相変調した信号をアンテナ18aから放射させ、路上機20との間のデータ通信を行う。

【0065】なお、発振器65及びトランジスタTr 1は、無変調の搬送波を送信してこないシステムの路上機との間のデータ通信をも実行できるようにするためのものであり、この場合、制御装置16は、トランジスタTr 1をオンして発振器65に電源供給を行い、発振器65から搬送波を出力させる。そして、この状態で、トランジスタTr 2及びトランジスタTr 3を送信すべきデータに応じて交互にオン・オフすることにより、発振器65からの搬送波をアンテナ18aから放射させる状態と、発振器65からの搬送波を遮断してアンテナ18aから信号を放射させない状態とに切り換える。つまり、このようにすることにより、発振器65からの搬送波を送信データに応じて振幅変調(ASK)した信号を、アンテナ18aから送信させるのである。

【0066】次に、本実施例の有料道路課金システムにおいて、車載機10と路上機20側の通信装置との間で

実行されるデータ通信、及びこのデータ通信のために車載機10側で実行されるデータ処理について説明する。但し、以下の説明は、路上機20が設けられた有料道路の入り口又は出口において支払うべき通行料金が一律である場合に車載機10及び路上機20において実行される処理であり、通行料金が走行距離や走行時間に応じて設定される場合とは若干異なる。

【0067】まず図4は、車載機10において、ICカードドライブ12の図示しない挿入口にICカード2が挿入された際に、制御装置16において送信データの準備のために実行されるデータ処理(カード挿入時処理)を表わすフローチャートである。なお、前述したように車載機10は通常スリープ状態にあるため、この処理は、ICカードドライブ12に設けられたセンサによりICカード2の挿入が検出され、その検出信号が制御装置16に入力されて、制御装置16が起動することにより開始される。

【0068】図4に示す如く、この処理が開始されると、制御装置16は、まずS110(S:ステップを表わす)にて、自らが正常動作するか否かを自己診断するダイアグノスチックテストを行い、S120にて、そのテスト結果が正常であるか否かを判定する。そして、テスト結果に異常があれば、ダイアグノスチックエラーとして、後述のS280に移行し、逆にテスト結果が正常であれば、S130に移行して、車載機10に電源供給している図示しないバッテリーの電圧を読み取るバッテリーチェックを行う。なお、バッテリーは、交換可能なバッテリーと、シールされたバッテリーとがあり、ここでは両方のバッテリーの電圧チェックを行う。

【0069】次にS140では、交換可能なバッテリーの電圧が極めて低く、バッテリー交換が必要であるか否かを判定し、バッテリー交換が必要であると判断されると、S150にて図示しない表示装置にその旨を表わす交換メッセージを表示した後、スリープ状態に入る。またS140にて、バッテリー交換の必要はないと判断されると、今度はS160にて、バッテリー電圧は、制御装置16及び通信回路18の動作には支障はないものの、ICカードドライブ12や暗号化モジュール14を動作させるには不十分な状態であるか否か(つまりバッテリー電圧は低いかどうか)を判定する。そして、バッテリー電圧が低い場合には、S170にて、電圧値等のバッテリー状態を表示装置に表示した後、バッテリーエラーとして、後述のS280に移行し、バッテリー電圧が正常であれば、S180に移行する。

【0070】なお、このバッテリーチェックにより、バッテリー交換が必要であったり、或はバッテリー電圧が低いことが判明した場合には、表示装置にその旨が表示されることから、車両乗員は、その表示内容からバッテリーの交換時期を知ることができ、バッテリーを交換することにより、車載機10を正常復帰させることができる。

【0071】次に、S180では、ICカードドライブ12を介してICカード2を起動（パワーオンリセット）し、ICカード2から、所定のカード情報を読み出し、ICカードドライブ12に装着されたICカード2は、当該車載機10において使用可能なカードかどうかをチェックする（ICカードチェック）。

【0072】そして、S190では、ICカードチェックの結果、ICカード2は当該車載機10において使用可能であるかを判定し、使用できない場合には、ICカードエラーとして、後述のS280に移行し、使用可能であれば、S200に移行して、暗号化モジュール14を起動し、ICカード2との間で相互認証させる。なお、この相互認証は、前述のDESアルゴリズムに従って生成した暗号化データを用いて後述の図5に示す手順で実行される。

【0073】次に、S210では、相互認証の結果、暗号化モジュール14及びICカード2は相手を互いに認証できたか否かを判定し、認証できなかった場合には、認証エラーとして、後述のS280に移行し、認証できた場合には、S220に移行する。

【0074】S220では、ICカード2が、予め通行料金を支払ってあるプリペイドカードであるか、或は、所定の銀行口座から通行料金を支払うキャッシュカードであるかを判定する。そして、ICカード2がキャッシュカードであれば、S230に移行して、ICカード2から、カードの有効期限や使用可能な車載機の制限事項の有無等、キャッシュカード特有のカード情報を読み出し、そのカード情報をチェック（キャッシュカードチェック）する。そして、続くS250にて、そのチェック結果から、キャッシュカードは使用可能であるか否かを判定し、使用できなければ、キャッシュカードエラーとして、後述のS280に移行し、逆に使用可能であれば、S270に移行する。

【0075】なお、このようにキャッシュカードには、カード情報として、使用可能な車載機の制限事項を記憶できるが、これはキャッシュカードを特定の車載機でのみ使用できるようにするためであり、制限事項としては、使用可能な車載機を特定する識別コード等が記憶される。

【0076】一方、ICカード2がプリペイドカードであれば、S240に移行して、ICカード2から、カードの有効期限や支払料金の残高等、プリペイドカード特有のカード情報を読み出し、そのカード情報をチェック（プリペイドカードチェック）する。そして、続くS260にて、そのチェック結果から、プリペイドカードは使用可能であったか否かを判定し、使用できなければ、プリペイドカードエラーとして、後述のS280に移行し、逆に使用可能であれば、S270に移行する。

【0077】S270では、ICカード2から通行料金を徴収してその結果（使用日時や残高等）を書き込むの

に必要な課金用鍵ZをICカード2から出力させて記憶する、課金用鍵Zの読込処理を行い、続くS290に移行する。即ち、ICカード2は、記憶したデータを容易に書き換えることができないように、データの更新には暗号化データを使用するようにされており、ここでは、カードデータ更新のための暗号化データを生成するのに必要な鍵（課金用鍵）ZをICカード2に生成させ、それを読取り、記憶した後、S290に移行するのである。なお、課金用鍵Zは、ICカード2に対して予め割り当てられたICカード固有の鍵（ICカード鍵）を用いて、カード処理回数等のカード情報をDESアルゴリズムに則って暗号化することにより生成される。

【0078】一方、S120、S160、S190、S210、S250、S260等で、車載機10或はICカード2の何等かのエラーが判定された場合には、S280にて、そのエラー内容を表わすエラーステータスをセットし、S290に移行する。

【0079】次に、S290では、路上機20側に送信するデータを暗号化するのに使用する鍵（通信用鍵X1）を暗号化モジュール14に生成させ、S300にて、その生成された通信用鍵X1を記憶する。なお、暗号化モジュール14は、制御装置16から通信用鍵X1の生成指令を受けると、まず乱数R1を発生し、その発生した乱数R1と数種類の中から選択可能な暗号鍵番号Knの通信マスタ鍵とを用いて、通信用鍵X1を生成する。また、この通信用鍵X1の生成には、DESアルゴリズムと比較して暗号化を高速に行うことのできる暗号化アルゴリズム（以下、FXアルゴリズムという）が使用される。

【0080】ここで、FXアルゴリズムとしては、スイス国のJ. L. MasseyのSAFER・K-64（Secure And Fast Encryption Routine of Length 64 bits）と呼ばれる暗号化アルゴリズムや、日本国のNTTのH. MatsumotoらのFEAL（Fast Data Encipherment Algorithm）が適している。

【0081】こうして通信用鍵X1が生成されると、今度は、S310にて、路上機20側に送信すべき車載機データ（第1リードデータ）RD1を読み込む。そして、続くS320では、暗号化モジュール14にこのデータRD1を出力して、上記生成した通信用鍵X1を用いて暗号化させる。なお、この暗号化にも上記FXアルゴリズムが使用される。

【0082】そして、暗号化モジュール14にて第1リードデータRD1が暗号化されると、S330にて、暗号化後の第1リードデータ<RD1>を、路上機20側への送信データとして記憶し、S340にて、上記280にてセットしたエラーステータスや、ICカード2から読み出したカード情報等に従いカード状態を車両乗員

に報知した後、スリープ状態に入る。

【0083】ここで、このカード状態の報知は、表示装置への表示及びブザーを用いた音声により同時に行う。つまり、ICカード2の種別や残金、或はカードの異常等を表示及び音声により報知することにより、車両乗員にカードの確認を促し、乗員が料金支払に使用するカードを確認して、異常等があれば交換できるようにする。

【0084】また、送信データとして記憶される第1リードデータRD1は、例えば図8に示す如く、路上機20側通信装置に対する応答コード、エラーステータス等の車載機10側の動作状態を表わすステータスコード、料金の支払方法等を表わす料金支払モード、車載機固有の車載機コード、ICカード2のシリアルナンバCSN、ICカード2の残高データ、ICカード2のシリアルナンバCSNとICカード2の種別を表わすアプリケーションナンバCANとのイクスクルーシブオア(CSN XOR CAN)、ICカード2内にて処理情報を記憶するメモリの最新位置を表わすトランザクションカウンタCTC、ICカード2側でカード情報をDESアルゴリズムに則って暗号化するのに用いられるICカード鍵の種別を表すインデックス(使用する鍵のインデックス)等から構成され、このうち、ステータスコード、料金支払モード、車載機コード、シリアルナンバCSN、及び、残高データの一部、が夫々暗号化され、それ以外は暗号化しない平文のまま送信データとして設定・記憶される。

【0085】次に、S200におけるICカード2と暗号化モジュール14との相互認証は、図5に示す如く実行される。なお、以下の図5に説明するICカード2及び暗号化モジュール14の動作において、各種データを生成する際には、全てDESアルゴリズムに則った関数が使用される。

【0086】即ち、図5に示す如く、この相互認証を行う際には、制御装置16が、まずICカード2から、シリアルナンバCSN、アプリケーションナンバCAN等のカード情報を出力させ(S31)、これを読み込む(S11)。そして、この読み込んだカード情報(CSN, CAN)を暗号化モジュール14に転送すると共に、暗号化モジュール14に乱数Rの生成指令を出力する(S12)。すると暗号化モジュール14は、この指令に従い乱数Rを生成する(S21)ので、制御装置16は、この乱数Rを読み込み、この乱数Rと共に認証用暗号鍵Yの生成指令をICカード2に出力する(S13)。

【0087】ICカード2は、認証用暗号鍵Yの生成指令を受けると、トランザクションカウンタCTCに対応したメモリ位置からカードデータを読み出し、このカードデータを、予め設定された前記ICカード鍵の一つである認証用鍵を用いて暗号化することにより認証用暗号鍵Yを生成し(S32)、更に、この認証用暗号鍵Yを

用いて乱数Rを暗号化する(S33)。

【0088】こうしてICカード2において乱数Rが暗号化されると、制御装置16はその暗号化データ<R>と認証用暗号鍵Yの生成に使用されたカードデータを読み出し、これら各データと共に、認証用暗号鍵Yの生成指令を暗号化モジュール14に出力する(S14)。

【0089】すると、暗号化モジュール14は、ICカード2のシリアルナンバCSNとアプリケーションナンバCANとのイクスクルーシブオア(CSN XOR CAN)を求め、これと所定のマスタ鍵とを用いてICカード2固有の認証用鍵を生成すると共に、この生成した認証用鍵とカードデータとを用いて認証用暗号鍵Yを生成し(S22)、更に、この認証用暗号鍵Yを用いて乱数Rを暗号化する(S23)。そして、暗号化モジュール14は、自らが暗号化した乱数Rの暗号化データ<R>'と、ICカード2側で暗号化された乱数Rの暗号化データ<R>とを比較し(S24)、これら各暗号化データが一致していれば、ICカードドライブ12に装着されたICカード2は正常であるとして認証する(S25)。なお、暗号化データが一致しなければ、制御装置16は、認証エラーと判定して、前記S280の処理に移行することになる。

【0090】こうして暗号化モジュール14側でのICカード2の認証が終了すると、制御装置16は、暗号化モジュール14に対して、ICカード2側で暗号化モジュール14を認証するための認証データを要求する(S15)。すると、暗号化モジュール14は、ICカード2のシリアルナンバCSNとアプリケーションナンバCANとのイクスクルーシブオア(CSN XOR CAN)と、所定のICカード鍵とを用いて、ICカード2が有する暗号化モジュール認証用の鍵SCを生成し、更にこの鍵SCをS22で生成した認証用暗号鍵Yを用いて暗号化することにより、認証データSC'を生成する(S26)。

【0091】そして、このように認証データSC'が生成されると、制御装置16は、この認証データSC'を読み込み、ICカード2に転送すると共に、ICカード2に認証指令を出力する(S16)。すると、ICカード2は、受け取った認証データSC'をS32で生成した認証用暗号鍵Yを用いて復号化し、その復号化した認証データSC' (= SC) が自らが有する鍵SCと一致するか否かを判定し(S34)、一致している場合に、ICカード2が装着された車載機10の暗号化モジュール14(換言すれば車載機10)は正常であると認証する(S35)。そしてこのようにICカード2側でも暗号化モジュール14が認証されると、制御装置16は相互認証は正常にできたとして(S17)、前述のS210からS220に移行し、逆にICカード2側にて暗号化モジュール14が認証されなければ、認証エラーとして、前記S280の処理に移行することになる。

【0092】次に、図6は、路上機20側の第1ガントリ30に設けられた通信装置32、34…にて各々実行される通信処理を表わすフローチャートである。なお、以下の説明においては、この通信処理を通信装置32が行うものとして説明する。図6に示す如く、通信装置32は、S410にて、スリープ状態にある車載機10を起動するための第1パイロット信号を送信し、その後、S420にて、所定期間T2、車載機10が応答信号を返送してくるための搬送波を送信しながら、アンテナ32aにて第1パイロット応答信号が受信されたか否かを判断し、第1パイロット応答信号が受信されなければ、再度S410に移行して、第1パイロット信号を送信する、といった手順で、第1パイロット信号を一定時間t[msec.]毎に送信する。

【0093】つまり、車両が第1ガントリ30付近まで走行してきて、車両が、走行中の車線に対応した通信装置32の通信エリア内に侵入すると、その車両に搭載された車載機10が、通信装置32からの第1パイロット信号を受信してスリープ状態から起動し、図7に示す如く、この第1パイロット信号に回答して第1パイロット応答信号を返送してくるため、上記S410及びS420では、第1パイロット信号を周期的に送信し、その送信により第1パイロット応答信号を受信できたか否かを判断することにより、車両が自己の通信エリア内に侵入してくるのを待つのである。

【0094】なお、図8に示す如く、第1ガントリ30において各通信装置32、34…が送信する第1パイロット信号は、車載機起動用のパイロット信号と、その送信元の通信装置を表わす場所番号とから構成され、この第1パイロット信号に回答して車載機10が送信する第1パイロット応答信号は、応答コードと、第1リードデータを生成した際に用いた通信用鍵X1の基となる乱数R1と通信マスタ鍵の鍵番号(暗号鍵番号)Knとから構成される。

【0095】こうして、車載機10から第1パイロット信号に回答して送信されてくる第1パイロット応答信号を受信すると、通信装置32は、S430に移行して、その第1パイロット応答信号に含まれる乱数R1及び暗号鍵番号Knと、通信用鍵X1の生成要求とを、暗号化ユニット32bに出力する。

【0096】すると、暗号化ユニット32bは、受け取った乱数R1及び暗号鍵番号Knに基づき、車載機10が第1リードデータ<RD1>を生成した際の通信用鍵X1をFXアルゴリズムに従って生成すると共に、車載機10が次の送信データ(第2リードデータ)を暗号化する際に用いる通信用鍵X2の基となる乱数R3及び通信マスタ鍵の鍵番号(暗号鍵番号)Kcを生成する。

【0097】そして、通信装置32は、S440にて、この生成された乱数R3及び暗号鍵番号Kcを読み出し、図7に示す如く、これら各値と第1リードデータの

読出指令とからなる路上機認証メッセージ(図8参照)を、車載機10側に送信する。なお、既述したように通信装置32は、この路上機認証メッセージを送信した際にも、その後所定期間T2、無変調の搬送波を送信する。また、通信装置32は、図7に示す如く、路上機認証メッセージや、後述の第1ライトデータ、エンドアック信号等の送信を、通常時の第1パイロット信号の送信と同様、一定時間t[msec.]毎に行う。

【0098】次に、上記のように路上機認証メッセージを車載機10側に送信すると、車載機10は、このメッセージに回答して、図7に示す如く、ICカード2の装着時に予め作成した第1リードデータ<RD1>を返送してくるため、通信装置32は、S450にて、その後、搬送波の送信期間T2が経過するまでの間、第1リードデータ<RD1>の受信を行い、搬送波の送信期間T2が経過すると、S460にて、この送信期間中に第1リードデータ<RD1>を受信できたか否かを判断することにより、通信エラーの発生の有無を判定する。

【0099】そして、通信エラーが発生した場合には、エラーステータスをセットした後、当該処理を一旦終了し、通信エラーが発生していなければ、S470に移行して、受信した第1リードデータ<RD1>の復号化要求を暗号化ユニット32bに出力する。暗号化ユニット32bは、第1リードデータ<RD1>の復号化要求を受け取ると、先に乱数R1と通信用の暗号鍵番号Kcとに基づき生成した通信用鍵X1を用いて、FXアルゴリズムに従い第1リードデータ<RD1>を復号化する。このため、通信装置32は、S470で第1リードデータ<RD1>の復号化要求を出力した後は、S480にて、その復号化データRD1を読み込む。

【0100】そして、S490にて、この復号化データRD1中のステータスコードに基づき、復号化した第1リードデータRD1にエラーがあるかどうかを判定し、データエラーが存在すれば、S540に移行し、第1リードデータRD1にデータエラーがなければ、S500に移行する。

【0101】S500では、第1リードデータRD1に基づき、車載機10側のICカード2は、プリペイドカードかキャッシュカードかを判定し、ICカード2がキャッシュカードであれば、S510に移行して、車載機コード等から車種を判別して、車種に応じた通行料金を計算した後、S550に移行する。一方、ICカード2がプリペイドカードであれば、S520に移行して、車載機コード等から車種を判別して、車種に応じた通行料金を計算し、続くS530にて、プリペイドカードの残高から通行料金を支払可能であるかどうかを判定する。そして、S530にて、プリペイドカードの残高は通行料金を支払可能であると判定されると、S550に移行し、プリペイドカードには通行料金を支払う残高がないと判断されると、S540に移行する。

【0102】なお、S540は、複号化した第1リードデータRD1にエラーがあったり、或はICカード2（詳しくはプリペイドカード）から料金を徴収できなかった場合に、その旨を表わすエラーデータを車載機10側に送信して知らせる共に、エラーステータスをセットするための処理であり、このエラー処理が終了すると、S590に移行する。

【0103】次に、S550では、車載機10側から通行料金を徴収するための第1ライトデータWD1を生成して、これを暗号化ユニット32bに出力することにより、暗号化ユニット32bに第1ライトデータWD1を暗号化させる。そして、暗号化ユニット32bにて第1ライトデータWD1が暗号化されると、その暗号化した第1ライトデータ<WD1>を読み込み、車載機10に送信する（図7参照）。なお、通信装置32は、この送信の際にも、第1ライトデータ<WD1>に対応した変調信号に続けて、所定期間T2、無変調の搬送波を送信する。

【0104】ここで、第1ライトデータWD1は、例えば図8に示す如く、車載機10側にてICカード2に通行料金の支払結果を書込ませるための書込命令と、車載機コードと、通行料金の総額と、当該通信装置32の場所番号と、料金徴収タイプの種別（つまり、均一料金徴収か、走行距離によって料金が変わるのか、時間によって料金が変わるのか）を表すトランザクションタイプと、年月日及び時刻とから構成され、このうち、車載機コードと料金総額と場所番号の一部とが夫々暗号化され、それ以外は暗号化しない平文のまま送信データ（第1ライトデータ<WD1>）として設定される。

【0105】また、暗号化ユニット32bは、この第1ライトデータWD1を暗号化する際には、上記生成した通信用鍵X1を用い、FXアルゴリズムに従って暗号化処理を行う。つまり、暗号化ユニット32b（34bも同じ）は、車載機10との通信にのみ使用されるものであるため、車載機10側の暗号化モジュール14とは異なり、通信用の暗号化アルゴリズムであるFXアルゴリズムのみを用いて、鍵の生成並びにデータの暗号化及び復号化を行う。

【0106】次に、車載機10は、送信した第1ライトデータ<WD1>を受信すると、図7に示す如く、その旨を表わす応答コードからなるエンド信号を送信して来るため、通信装置32は、第1ライトデータ<WD1>の送信後、所定期間T2、このエンド信号を受信する処理（S570）を行い、所定期間T2経過後、S580にて、エンド信号を受信できたか否かを判定することにより、通信エラーの有無を判定する。そして、通信エラーが発生した場合には、エラーステータスをセットした後、当該処理を一旦終了し、通信エラーが発生していなければ、S590に移行する。

【0107】そして、S590では、上記復号化した第

1リードデータRD1やエラー処理（S540）においてセットされたエラーステータス等を、路上機20本体に内蔵されたローカルコントローラ26に出力し、続くS600にて、車載機10に対してデータ通信が完了したことを知らせる通信完了信号としてのエンドアック信号及び第1パイロット信号を送信し（図7参照）、当該処理を一旦終了する。

【0108】なお、このようにエンドアック信号に続けて第1パイロット信号を送信するのは、通信エリアに次に侵入してきた車両に搭載された車載機10を速やかに起動させるためであり、これによって、車載機10の起動が遅れて、通信時間が短くなるのを防止できる。

【0109】また、S600にて第1パイロット信号を送信した後は、上記S420と同様の図示しない判定処理にて、第1パイロット信号に応答して車載機10側から第1パイロット応答信号が送信されてきたかどうかを判定し、第1パイロット応答信号を受信すると、上記S430に移行して、その第1パイロット応答信号を送信してきた車載機との間の通信を開始し、第1パイロット応答信号を受信できなければ、S410に移行して、第1パイロット信号を一定時間t[msec.]毎に送信する通常動作に戻る。

【0110】次に、図9は、車載機10が、第1ガントリ30に設けられた通信装置32、34…からの第1パイロット信号を受けて起動し、第1パイロット信号を送信してきた通信装置との間で、上述した手順で通信処理を行った後に、車載機10において実行されるデータ処理（第1ガントリ通過処理）を表わすフローチャートである。

【0111】図9に示す如く、車載機10においては、通信回路18が、第1ガントリ30の通信装置、例えば通信装置32からの第1パイロット信号を受信することにより、制御装置16を起動し、その後、制御装置16は、通信回路18を介して、通信装置32との間でデータ通信を行う通信処理（610）を実行する。そして、制御装置16は、通信装置32からの第1ライトデータ<WD1>を受信すると、通信回路18を介してエンド信号を送信して、通信処理（S610）を終了し、S620以降の第1ガントリ通過処理を実行する。

【0112】S620においては、通信装置32からのエンドアック信号を受信したかどうかを判定する。そして、エンドアック信号を受信できていない場合には、S630に移行し、通信回路18を介して、その後通信装置32が一定時間t[msec.]毎に送信する第1パイロット信号或は他の車載機10に対する送信信号に続く無変調の搬送波を利用して、エンドアック信号の要求信号を送信する。

【0113】また、続くS640では、通信回路18にて、通信装置32からの第1パイロット信号等の送信信号を受信できているかどうか、換言すれば、車両が通信

装置32の通信エリアを脱出したかどうかを判定し、車両が通信エリア内にいれば、再度S620に移行して、通信装置32が上記要求信号に応答して、エンドアック信号を送信してきたかどうかを判定する。

【0114】そして、エンドアック信号を受信できなければ再度S630に移行し、その後は、車両が通信装置32の通信エリアから脱出するか、エンドアック信号を受信できるまでの間、S620～S640の処理を繰り返す。つまり、第1ガントリ30の通過時に、通信装置32との間の通信を完了した後、エンドアック信号を受信できない場合には、エンドアック信号の要求信号を通信装置32に送信して、エンドアック信号を再送信させるのである。

【0115】この結果、車載機10側では、通信装置32との通信完了を確実に確認できるようになり、もしエンドアック信号を受信できなかった場合でも、その旨を通信装置32を介して路上機20側に知らせることができ、通信エラーを相互で確認できるようになる。

【0116】こうして、エンドアック信号を受信するか、車両が第1ガントリ30の通信装置32、34…の通信エリアを脱出すると、S650に移行して、暗号化モジュール14に対し、路上機20側から受け取った第1ライトデータ<WD1>の復号化指令を出力する。すると、暗号化モジュール14は、第1ライトデータ<WD1>を、通信用鍵X1を用いて、FXアルゴリズムに従い復号化するので、続くS660では、この復号化された第1ライトデータWD1を読み出し、この第1ライトデータWD1に含まれる車載機コードと、当該車載機10の車載機コードとに基づき、路上機20（詳しくは第1ライトデータWD1を送信してきた通信装置）を認証する。

【0117】そして、S670では、S660にて路上機20を認証できたかどうかを判定し、上記各車載機コードが一致しておらず路上機を認証できなければ、S680にてその旨を表わすエラーステータスをセットした後、スリープ状態に入り、上記各車載機コードが一致しており路上機20を認証できた場合には、S690に移行する。

【0118】S690では、先のデータ通信時に路上機20側から受け取った乱数R3及び暗号鍵番号Kcを暗号化モジュール14に転送することにより、次のデータ通信に使用する通信用鍵X2を生成させ、通信用鍵をX1からX2に変更する。なお、暗号化モジュール14は、乱数R3及び暗号鍵番号Kcを受け取ると、乱数R3及び暗号鍵番号Kcに対応した通信マスタ鍵とを用いて、FXアルゴリズムに従って通信用鍵X2を生成する。

【0119】こうして通信用鍵をX1からX2に変更すると、今度はS700にて、ICカード2の種別を判定し、ICカード2がプリペイドカードであれば、S71

0にて、プリペイドカードは通行料金を支払うだけの残高があるかどうかを判定する。そして残高がなければ、S720にて課金金額を零に設定して、S730に移行し、通行料金を支払うことができれば、そのままS730に移行する。

【0120】S730では、プリペイドカードであるICカード2から通行料金を差し引くための課金処理を行い、S740にて、ICカード2から通行料金を正常に差し引くことができたか否かを判定する。そして、プリペイドカードから通行料金を差し引くことができなかった場合、つまりプリペイドカードに残高がなかったり、或は課金処理を正常に実行できなかった場合には、S750に移行して、その旨を表わすエラーステータスをセットした後、スリープ状態に入り、逆に通行料金を正常に差し引くことができた場合には、S780に移行する。

【0121】またS700にて、ICカード2はキャッシュカードであると判断された場合には、S760に移行して、キャッシュカードから通行料金を支払うための口座情報を読み出し、S770にて、その読み出した口座情報は正常であるか否かを判断する。そして、口座情報が正常でなければ、そのままスリープ状態に入り、口座情報が正常であれば、S780に移行する。

【0122】次に、S780では、路上機20側に次に送信すべき車載機データ（第2リードデータ）RD2を暗号化モジュール14に出力して、この第2リードデータRD2を、S690にて変更した通信用鍵X2を用いて暗号化させる。なお、この暗号化にも上記FXアルゴリズムが使用される。そして、暗号化モジュール14にて第2リードデータRD2が暗号化されると、S790にて、その暗号化後のデータ<RD2>を、次の送信データとして記憶し、S800にて、ICカード2に通行料金を支払った日付、時間、場所等の支払情報を書込み、カードデータを更新し、S810にて、その更新後のカード情報を読み込み、記憶した後、スリープ状態に入る。

【0123】ここで、プリペイドカードから通行料金を差し引く課金処理（S730）や、ICカード2のデータを更新するカードデータ更新処理（S800）は、前述のS270にて予め記憶した課金用鍵Zを用い、DESアルゴリズムに従って暗号化したデータを用いて行われる。

【0124】そして、S780にて暗号化され、S790にて送信データとして記憶される第2リードデータRD2は、例えば図12に示す如く、路上機20側通信装置に対する応答コード、ICカード2がキャッシュカードである場合のキャッシュカードファイル情報（口座情報等）、エラーステータス等の車載機10側の動作状態を表わすステータスコード、支払方法、通行料金の徴収結果、車載機コード、ICカード2のアプリケーション

ナンバCAN、乱数R3、車載機10側で料金を徴収できたことを証明する料金徴収証明データ等から構成され、この内、応答コードとキャッシュカードファイル情報の一部とが暗号化されずに平文のまま残され、残りのデータは全て暗号化される。

【0125】なお、このように第2リードデータRD2は、第1リードデータRD2と同様、FXアルゴリズムに従って暗号化されるが、この内、料金徴収証明データは、ICカード2側でICカード鍵を用いてDESアルゴリズムに則って既に暗号化されており、送信時には更にFXアルゴリズムに則って暗号化することにより、2重の暗号化が施されることになる。

【0126】次に、図10は、路上機20の第2ガントリ40に設けられた通信装置42、44…にて各々実行される通信処理を表わすフローチャートである。なお、以下の説明においては、この通信処理を通信装置42が行うものとして説明する。図10に示す如く、通信装置42は、第1ガントリ30の通信装置32、34…と同様、S910にて、スリープ状態にある車載機10を起動するための第2パイロット信号を送信し、S920にて、所定期間T2、車載機10が応答信号を返送してくるための搬送波を送信しながら、アンテナ42aにて第2パイロット応答信号が受信されたか否かを判断し、第2パイロット応答信号が受信されなければ、再度S910に移行して、第2パイロット信号を送信する、といった手順で、第2パイロット信号を一定時間t[msec.]毎に送信する。

【0127】そして、車載機10が第2パイロット信号を受信してスリープ状態から起動し、図11に示す如く、この第2パイロット信号に応答して第2パイロット応答信号を返送してくると、この応答信号を受信して、S930に移行し、このパイロット応答信号に基づき、車載機10側のICカード2の種別を判定する。つまり、車載機10は、第2パイロット信号を受信すると、第2パイロット応答信号として、応答コードと料金の支払方法を表わす支払モードデータを返送する(図12参照)ようにされているため、ここでは、この支払モードデータから、車載機10側のICカード2がキャッシュカードかプリペイドカードかを判定するのである。

【0128】そして、ICカード2がプリペイドカードであれば、そのままS950に移行し、ICカード2がキャッシュカードであれば、路上機20の本体側に設けられたローカルコントローラ26に対して、車載機10に伝えるべき表示メッセージを検索するよう指令を出した後、S950に移行する。なお、この表示メッセージの検索指令により、ローカルコントローラ26は、キャッシュカードの利用状況等を検索して、車載機10側に伝えるべき表示メッセージを生成し、通信装置42に送信する(図11参照)。

【0129】次にS950では、車載機10に対して、

第2リードデータ<RD2>を要求するデータ読み出し信号を送信し、その後、S960にて、所定期間T2、無変調の搬送波を送信しながら、車載機10から第2リードデータ<RD2>が送信されてくるのを待つ受信処理を行い、所定期間T2経過すると、S970にて、第2リードデータ<RD2>を受信できたか否かを判断することにより、通信エラーの発生の有無を判定する。そして、通信エラーが発生した場合には、エラーステータスをセットした後、当該処理を一旦終了する。

【0130】一方、S950にて送信したデータ読み出し信号に応答して、車載機10が第2リードデータ<RD2>を返送してくると、S980に移行して、第2ガントリ40側で第2リードデータ<RD2>を受け取った旨を車載機10側に記憶・表示させるための書込命令・表示命令や、ICカード2がキャッシュカードの場合にローカルコントローラ26側にて検索・生成された表示メッセージ等からなる第2ライトデータWD2(図12参照)を生成して、車載機10に送信する。

【0131】車載機10は、第2ライトデータWD2を受信すると、図11に示すように、応答コードからなるエンド信号を送信してくるため、続くS990では、所定期間T2、無変調の搬送波を送信しながら、車載機10からエンド信号が送信されてくるのを待つ受信処理を行い、所定期間T2経過すると、S1000にて、エンド信号を受信できたか否かを判断することにより、通信エラーの発生の有無を判定する。

【0132】そして、通信エラーが発生した場合には、エラーステータスをセットした後、当該処理を一旦終了し、通信エラーが発生していなければ、S1010にて、車載機10から受け取った車載機データ、つまり第2リードデータ<RD2>を、ローカルコントローラ26へ転送し、続くS1020にて、エンドアック信号と第2パイロット信号とを送信し(図11参照)、当該処理を一旦終了する。

【0133】なお、S1020にて第2パイロット信号を送信した後は、第1ガントリ30における各通信装置32、34…の処理と同様、上記S920と同様の図示しない判定処理にて、第2パイロット信号に応答して車載機10側から第2パイロット応答信号が送信されてきたかどうかを判定し、第2パイロット応答信号を受信すると、上記S930に移行し、第2パイロット応答信号を受信できなければS910に移行する。

【0134】また、S1010においてローカルコントローラ26へ転送される第2リードデータ<RD2>は、FXアルゴリズムに従い暗号化した暗号化データであり、その内の料金徴収証明データは、更にDESアルゴリズムにて暗号化されているため、ローカルコントローラ26側にて、内蔵した暗号化ユニットを用いて復号化される。そして、このときFXアルゴリズムにて復号化した料金徴収証明データを更にDESアルゴリズムに

て復号化するには、第1ガントリ30において車載機10側から受信した第1リードデータRD1中の鍵のインデックスを利用して、車載機10に搭載されたICカード固有のICカード鍵を求め、これから復号化用の暗号鍵を生成する、といった手順でICカード2が料金徴収証明データを暗号化した際の暗号化鍵を求め、これを用いて料金徴収証明データを復号化する。次に、図13は、車載機10が、第2ガントリ40に設けられた通信装置42、44…からの第2パイロット信号を受けて起動し、第2パイロット信号を送信してきた通信装置との間で、上述した手順で通信処理を行った後に、車載機10の制御装置16において実行されるデータ処理（第2ガントリ通過処理）を表わすフローチャートである。

【0135】図13に示す如く、制御装置16は、第2ガントリ40の通信装置42、44…との間のデータ通信により、第2ライトデータWD2を受信し、エンド信号を送信して、通信処理（S1110）を終了すると、第1ガントリ30における通信処理終了時と同様、エンドアック信号を受信したかどうかを判定し（S1120）、エンドアック信号を受信できなければ、通信装置42、44…が送信してくる無変調の搬送波を利用してエンドアック信号の要求信号を送信し（S1130）、更に、車両が第2ガントリ40の通信エリアを脱出したかどうかを判定し（S1140）、車両がこの通信エリア内にいれば再度S1120に移行する、といった手順で、通信処理（S1110）終了後、車両が第2ガントリ40の通信エリアから脱出するか、エンドアック信号を受信できるまでの間、S1120～S1140の処理を繰り返す。

【0136】そして、エンドアック信号を受信するか、車両が第2ガントリ40の通信エリアを脱出すると、S1150に移行して、前述のS290と同様、次に送信データを暗号化するための通信用鍵X1を暗号化モジュール14に再度生成させ、S1160にて、その生成された通信用鍵X1を記憶する。また続くS1170では、次に路上機20側に送信すべき車載機データ（第1リードデータ）RD1を読み込んで、暗号化モジュール14に、上記生成した通信用鍵X1を用いて暗号化させ、S1180にて、その暗号化された第1リードデータ<RD1>を記憶する。なお、暗号化モジュールにおける通信用鍵X1の生成及び第1リードデータRD1の暗号化の手順は、ICカード2がICカードドライブ12に装着されたときと全く同様であり、異なる点は、第1リードデータRD1とされる車載機データのうち、ICカード2に関するデータ内容が、前記S810にて記憶された課金後の内容に変更されている点だけである。

【0137】そして、このように暗号化した第1リードデータ<RD1>を記憶すると、続くS1190において、車載機10の状態をエラー発生時にセットされるエラーステータス等からチェックし、何等かのエラーがあ

れば、S1130に移行して、その旨をブザー等を用いて報知し、エラーがなければ、S1120に移行して、カード状態をブザー及び表示装置にて報知した後、スリープ状態に入る。なお、カード状態の表示内容は、ICカード2がプリペイドカードであれば、カード残高等であり、ICカード2がキャッシュカードであれば、使用金額や第2ライトデータWD2に含まれる表示メッセージ等である。

【0138】次に図14は、車載機10において、ICカードドライブ12からICカード2が抜き取られた場合に、制御装置16にて実行されるデータ処理（カード抜取時処理）を表わすフローチャートである。なお、この処理は、ICカードドライブ12に設けられたセンサによりICカード2の抜き取りが検出され、その検出信号が制御装置16に入力されて、制御装置16が起動することにより開始される。

【0139】図14に示す如く、この処理が開始されると、制御装置16は、まずS1210において、ICカード2が抜き取られ、当該車載機10には通行料金を支払うためのカードがない旨を表わすエラーステータスをセットする。そして、続くS1220では、現在記憶されている暗号化後の第1リードデータ<RD1>をセットしたエラーステータスに対応した内容に更新すべく、エラーステータスセット後の車載機データを読み込み、これを暗号化モジュール14に出力して、暗号化した第1リードデータ<RD1>を新たに生成させる。

【0140】そして、暗号化モジュール14にて第1リードデータ<RD1>が生成されると、S1230にて、この生成された第1リードデータ<RD1>を次に路上機20側に送信すべき送信データとしてこのデータを更新し、S1240にて、抜き取られたICカード2の使用状態等を表示した後、スリープ状態に入る。

【0141】以上説明したように、本実施例の有料道路課金システムにおいては、車載機10が送信データの暗号化及び受信データの復号化を行うのは、料金支払のためのICカード2がICカードドライブ12に装着されたときと、路上機20側の第1ガントリ30に設けられた通信装置32、34…との間で通信処理を行ってから、第2ガントリ40に設けられた通信装置42、44…の通信エリアに入るまでの間と、第2ガントリ40の通信装置32、34…との間で通信処理を行った後と、ICカード2がICカードドライブ12から取り外されたときであり、路上機20側通信装置32、34…、42、44…との間の通信中には、暗号化も復号化も共に実行しない。また同様に、ICカード2からのカード情報の読出し、及びカードデータの更新についても、路上機20側通信装置32、34…、42、44…との間の通信中には実行しない。

【0142】このため、車載機10ー路上機20間でのデータ通信時に車載機10側で費やされる処理時間を極

めて短くすることができ、データ通信に必要な時間を短くできる。従って、車両の走行速度を制限したり、暗号化モジュール14を高速処理が可能な高価なものに変更することなく、データ通信を短時間で正確に行うことが可能になる。

【0143】また車載機10は、ICカード2がICカードドライブ12に装着されると、ICカード2と暗号化モジュール14との相互認証を行い、その認証結果を表わすステータス情報（エラーステータス）を車載機データのの一つとして路上機20側に送信するため、ICカード2や車載機10自体が偽造された場合には、路上機20側でその旨を検出することができる。従って、車両乗員の不正を抑制して、料金徴収を良好に行うことができる。

【0144】また、こうした相互認証やICカード2へのデータの書き込みを行う際には、従来より一般に使用されているDESアルゴリズムに則った暗号化データが使用されるが、車載機10－路上機20間の通信には、DESアルゴリズムとは異なり、しかもDESアルゴリズムよりも高速に暗号化を行うことのできるFXアルゴリズムにて暗号化した暗号化データを使用するようにされている。

【0145】このため、第1ガントリ30に設けられた通信装置32、34…において、データ通信中に送信データの暗号化及び受信データの復号化を行うのに要する処理時間を短縮することができ、データ通信をより高速且つ正確に行うことができる。また特に、FXアルゴリズムに、前述のSAFER・K-64或はFEALと呼ばれる暗号化アルゴリズムを用いれば、暗号化ユニットをハード構成にて比較的安価に実現でき、暗号化に要する時間をより短くすることができるため、より効果的である。

【0146】また、このように本実施例では、車載機10と路上機20側通信装置との間のデータ通信に、一般に使用されているDESアルゴリズムとは異なるFXアルゴリズムを使用するため、通信信号が傍受されても、復号化し難くし、通信の機密性を向上できる。そして特に、本実施例では、送信データを暗号化するに当たって、データの全文を暗号化するのではなく、その一部は平文のまま残すようにし、しかも、通信用鍵（X1、X2）は使用の度に、乱数を発生させてその乱数に従い更新するので、そのデータを、より復号化し難くなり、通信の機密性をより向上できる。

【0147】また、通信用鍵X1、X2は、車載機10と路上機20側通信装置とで各々設定されるため、正規の車載機10からの送信信号をそのままコピーした信号を発生する発信機を用いて、通行料金を不正に支払おうとしても、その不正を路上機20側で確実に検出することができ、安全性を向上できる。

【0148】一方、本実施例では、上記相互認証の結果

等、車載機10側で生じたエラーについては全てエラーステータスとして、路上機20側に送信され、また路上機20側にてエラーを検出した場合にも、車載機10に送信するようにされているため、車載機10と路上機20とで互いに異常を知ることができ、車載機10及び路上機20側で、夫々、エラー対策を行うことができる。

【0149】以上、本発明の一実施例について説明したが、本発明は、こうした実施例に限定されるものではなく、種々の態様をとることができる。例えば上記実施例では、有料道路の入り口又は出口に設けられた路上機20が、車載機10との間のデータ通信により、車種によって異なるものの走行距離や走行時間に対しては一律の通行料金を徴収する場合について説明したが、走行距離や走行時間に応じて通行料金を設定する有料道路課金システムにも本発明を適用できるのはいうまでもない。

【0150】そして、この場合、有料道路の出口において、走行距離や走行時間に応じた通行料金を徴収できるようにするために、有料道路の入り口に第1ガントリ30と同様に構成された入り口ガントリを設けて、ここを通過する車両に搭載された車載機10との間で、図15に示す如き構成の信号を送受信し、更に有料道路の出口に、第1ガントリ30及び第2ガントリ40と同様の構成の出口第1ガントリ及び出口第2ガントリを設けて、各ガントリを通過する車両に搭載された車載機10との間で、図16及び前記実施例にて説明した図12に示す如き構成の信号を送受信して、通行料金を徴収するようにすればよい。

【0151】即ち、図15に示す如く、車載機10側にて、応答コード、ステータスコード、料金支払モード、車載機コード等からなる入り口リードデータを予め生成・暗号化して、記憶しておき、車両が入り口ガントリに設けられた通信装置の通信エリアに入ったときに、その通信装置から周期的に送信される入り口パイロット信号により起動して、前記実施例の第1パイロット応答信号（図8参照）と同様に構成された入り口パイロット応答信号を送信し、その後、入り口ガントリの通信装置からデータ読み出し信号が送信されてきたときに、入り口リードデータを送信し、一方、入り口ガントリの通信装置では、入り口リードデータ受信後、前記実施例の第1ライトデータ（図8参照）から料金総額を除去した構成の入り口ライトデータを送信し、その後、エンド信号及びエンドアック信号の送受信を行い、データ通信を完了するように構成する。

【0152】また、こうして車両が入り口ガントリを通過した後は、図16に示す如く、車載機10側にて、出口第1ガントリを通過する際に送信すべきデータとして、応答コード、車載機コード、入り口場所番号、入場年月日、入場時刻等からなる入り口データと、前記実施例の第1リードデータと同様に構成された第1リードデータとを、夫々、生成・暗号化して記憶し、車両が出口

第1ガントリに設けられた通信装置の通信エリアに入ったときに、その通信装置から周期的に送信される第1パイロット信号により起動して、入り口パイロット応答信号と同様に構成された第1パイロット応答信号を送信し、その後、出口第1ガントリの通信装置から送信されてくる、応答コード、乱数R3、暗号鍵番号Kcからなる路上機認証メッセージを受信して、入り口データを送信し、更にその後路上機側通信装置から送信されてくるデータ読み出し信号を受信して、第1リードデータを送信し、一方、出口第1ガントリの通信装置では、この第1リードデータを受信すると、前記実施例の第1ライトデータに、入り口ガントリ通過後の走行時間又は出口番号からなる課金用データを追加した第1ライトデータを送信し、その後、エンド信号及びエンドアック信号の送受信を行い、データ通信を完了するように構成する。

【0153】また次に、車両が出口第1ガントリを通過した後は、図12に示したように、車載機10側にて、出口第2ガントリを通過する際に送信すべきデータとして、前記実施例の第2リードデータと同様のデータを生成・暗号化して記憶し、車両が出口第2ガントリに設けられた通信装置の通信エリアに入ると、その通信装置と車載機10との間で、前記実施例の第2ガントリ40通過の際と同様のデータ通信を行い、その後、通信結果をICカード2に書込むように構成する。

【0154】そして、このようにすれば、通行料金を走行距離に応じて設定するシステムでも、走行時間に応じて設定するシステムでも、有料道路の出口において、ICカード2から通行料金を自動徴収することができる。また、通行料金を走行距離に応じて設定するシステムと、走行時間に応じて設定するシステムとで異なる点は、図16に示す第1ライトデータにおける課金用データを、走行時間にするか或は走行距離が解る出口番号にするかの点のみであり、車載機と路上機側とで送受信するデータの構成及び送受信パターンは、全く同様であるため、これら両システムで、車載機10を共用することができるようになる。

【図面の簡単な説明】

【図1】 実施例の有料道路課金システム全体構成を表わすブロック図である。

【図2】 車載機の通信回路の構成を表わす電気回路図である。

【図3】 路上機側通信装置が送信する送信信号を説明する説明図である。

【図4】 車載機において実行されるカード挿入時処理を表わすフローチャートである。

【図5】 車載機側にてICカードと暗号化モジュールとの相互認証を行う際の手順を表わす説明図である。

【図6】 第1ガントリに設けられた通信装置にて実行される通信処理を表わすフローチャートである。

【図7】 第1ガントリに設けられた通信装置と車載機との間のデータ通信の流れを説明する説明図である。

【図8】 図7に示すデータ通信時に送受信されるデータの構成を説明する説明図である。

【図9】 車載機において実行される第1ガントリ通過処理を表わすフローチャートである。

【図10】 第2ガントリに設けられた通信装置にて実行される通信処理を表わすフローチャートである。

【図11】 第2ガントリに設けられた通信装置と車載機との間のデータ通信の流れを説明する説明図である。

【図12】 図11に示すデータ通信時に送受信されるデータの構成を説明する説明図である。

【図13】 車載機において実行される第2ガントリ通過処理を表わすフローチャートである。

【図14】 車載機において実行されるカード抜取時処理を表わすフローチャートである。

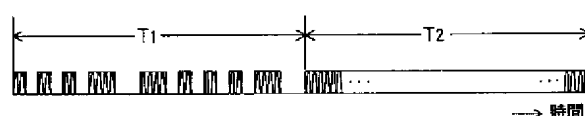
【図15】 距離又は時間に応じて通行料金を設定するシステムにおいて入り口ガントリにて送受信されるデータの構成を説明する説明図である。

【図16】 距離又は時間に応じて通行料金を設定するシステムにおいて出口第1ガントリにて送受信されるデータの構成を説明する説明図である。

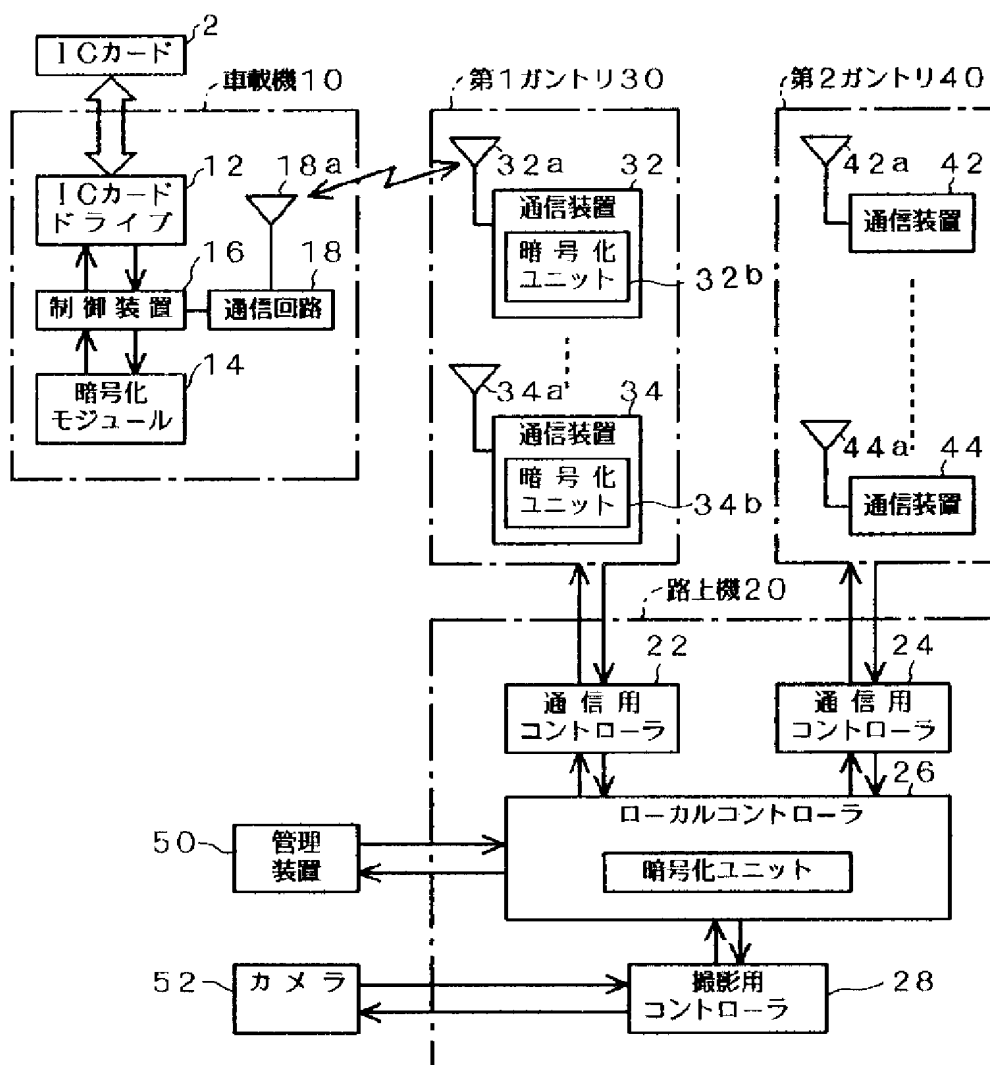
【符号の説明】

2…ICカード      10…車載機      12…ICカードドライブ  
14…暗号化モジュール      16…制御装置      18…通信回路  
18a…アンテナ      20…路上機      22…通信用コントローラ  
26…ローカルコントローラ      28…撮影用コントローラ  
30…第1ガントリ      32, 34…通信装置  
32a, 34a…アンテナ      32b, 34b…暗号化ユニット  
40…第2ガントリ      42, 44…通信装置  
42a, 44a…アンテナ      50…管理装置      52…カメラ

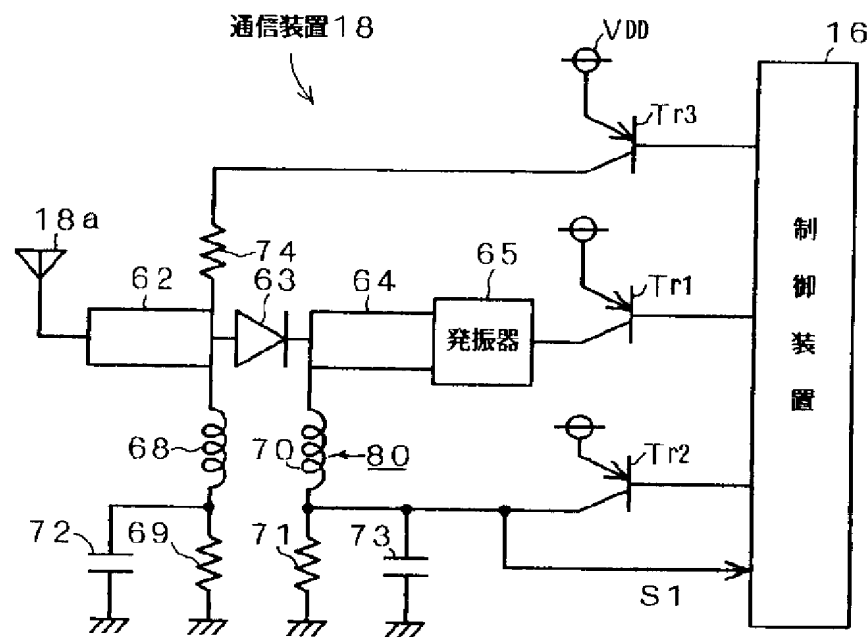
【図3】



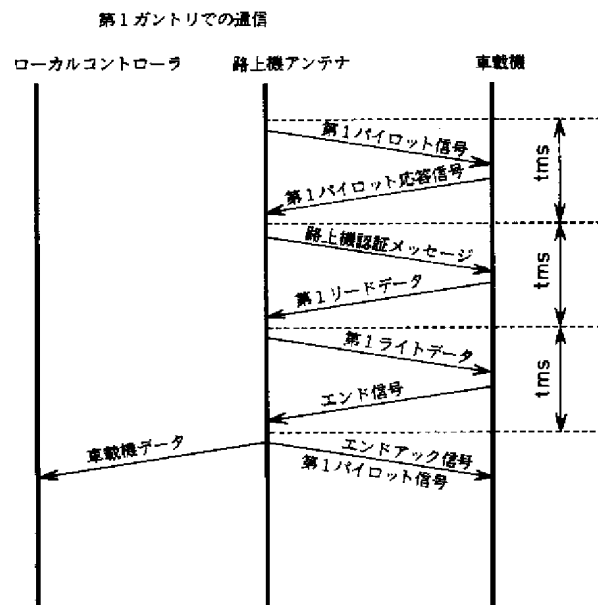
【図1】



【図2】



【図7】

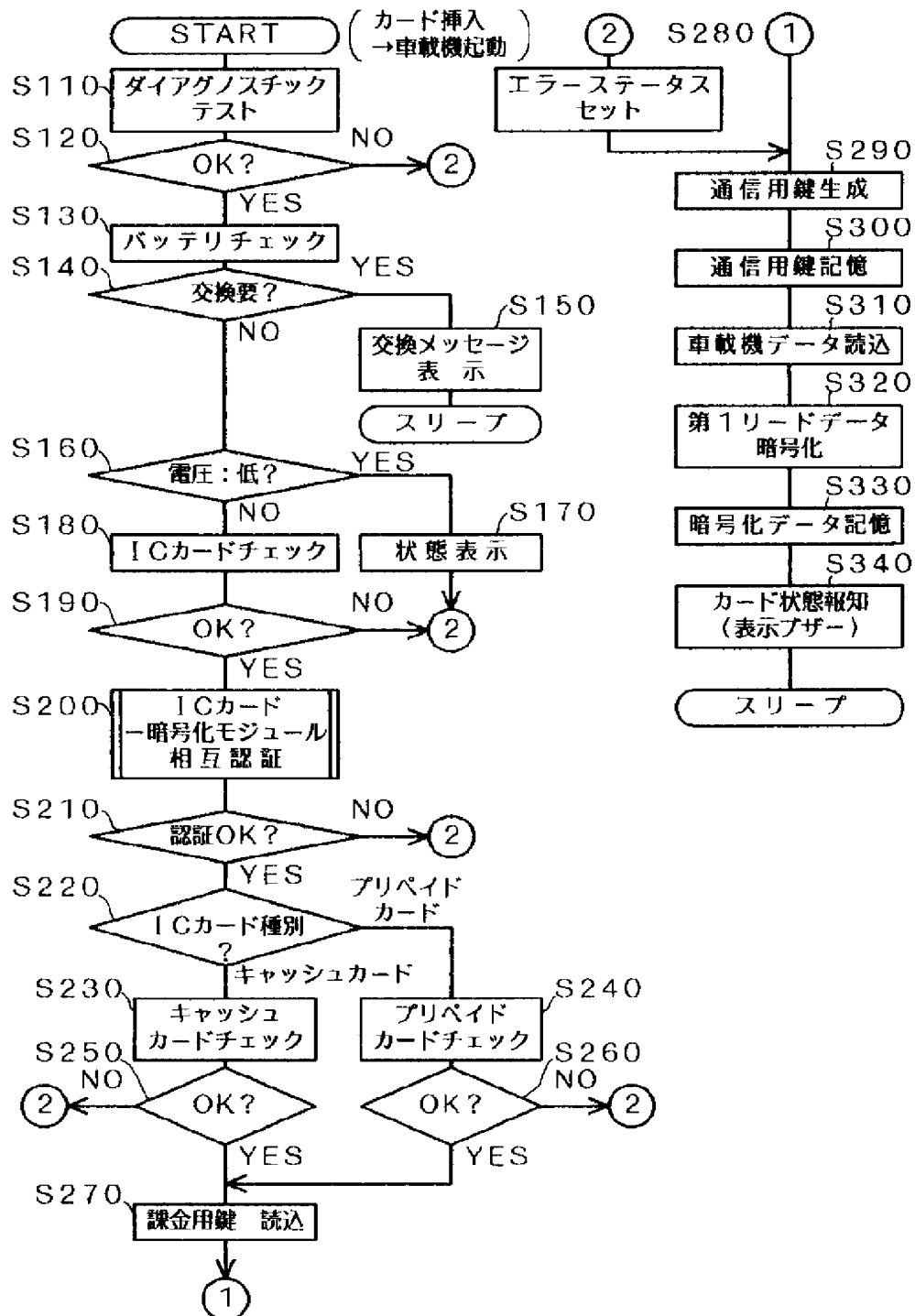


【図8】

第1ガントリでの通信信号	内 容
第1パイロット信号 (路上機)	パイロット信号 場所番号
第1パイロット応答信号 (車載機)	応答コード 乱数 R1 暗号鍵番号 Kn
路上機認証メッセージ (路上機)	データ読み出し命令 乱数 R3 暗号鍵番号 Kc
第1リードデータ (車載機)	応答コード ④ステータスコード (エラーコード) ④料金支払モード ④車載機コード ④CAN ④残高データ (途中まで暗号化) CSN XOR CAN CTC 使用する鍵のインデックス
第1ライトデータ (路上機)	書込命令 #車載機コード #料金総額 #場所番号 (途中まで暗号化) トランザクションタイプ 年月日 時刻
エンド信号 (車載機)	応答コード
エンドアック信号 (路上機)	END ACK

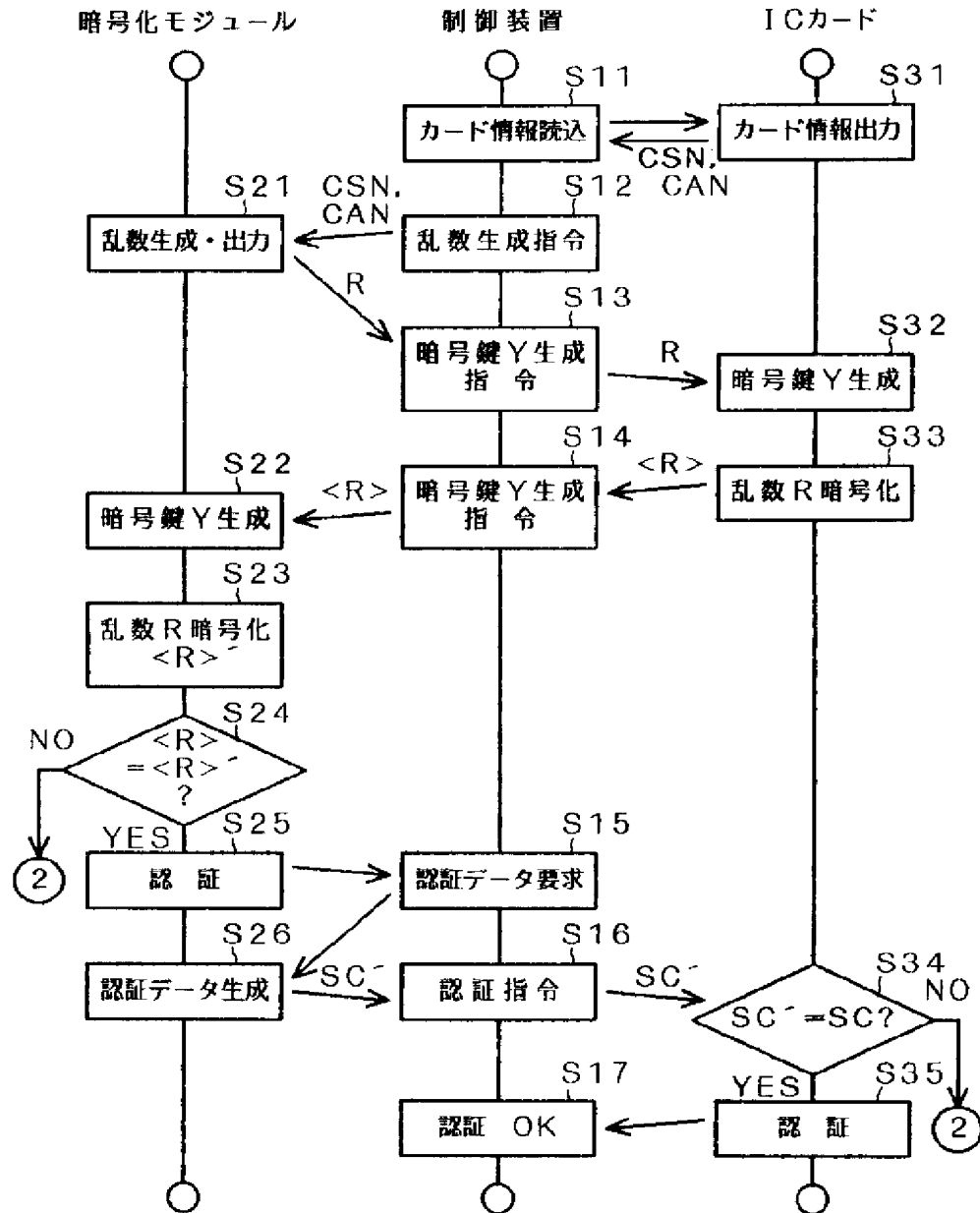
④ 車載機で暗号化されるデータ # 路上機で暗号化されるデータ

【図4】

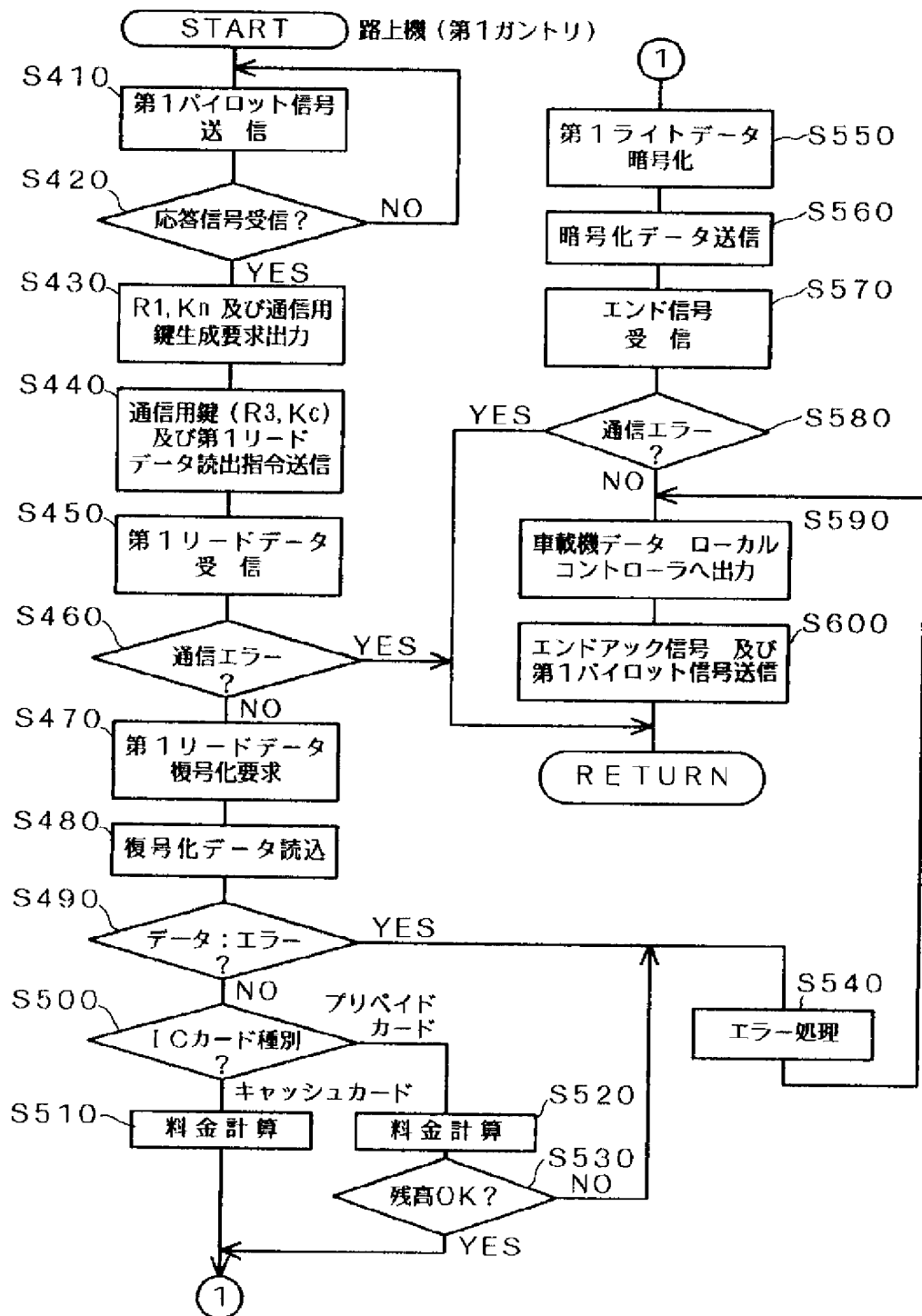


【図5】

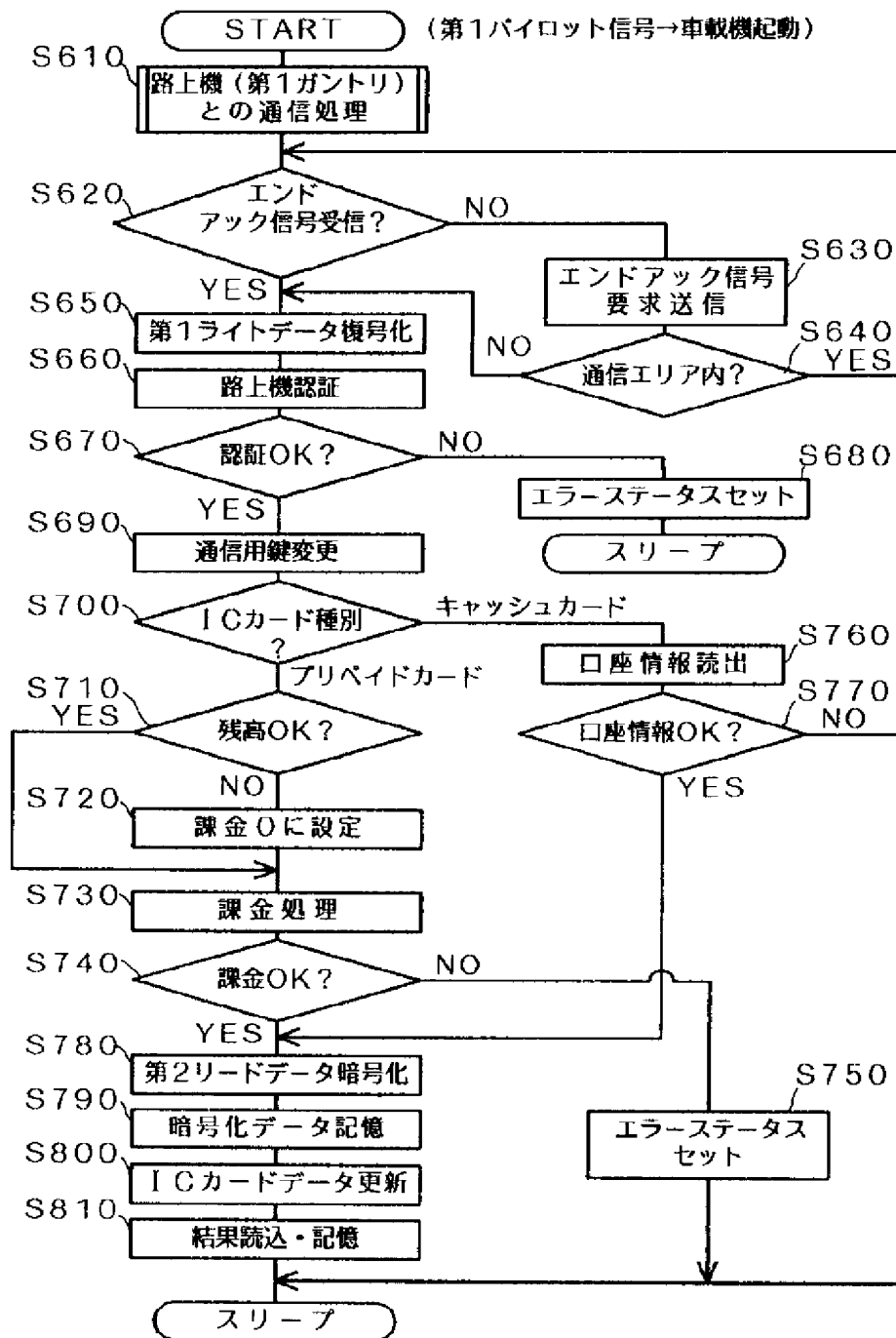
(ICカード-暗号化モジュール相互認証)



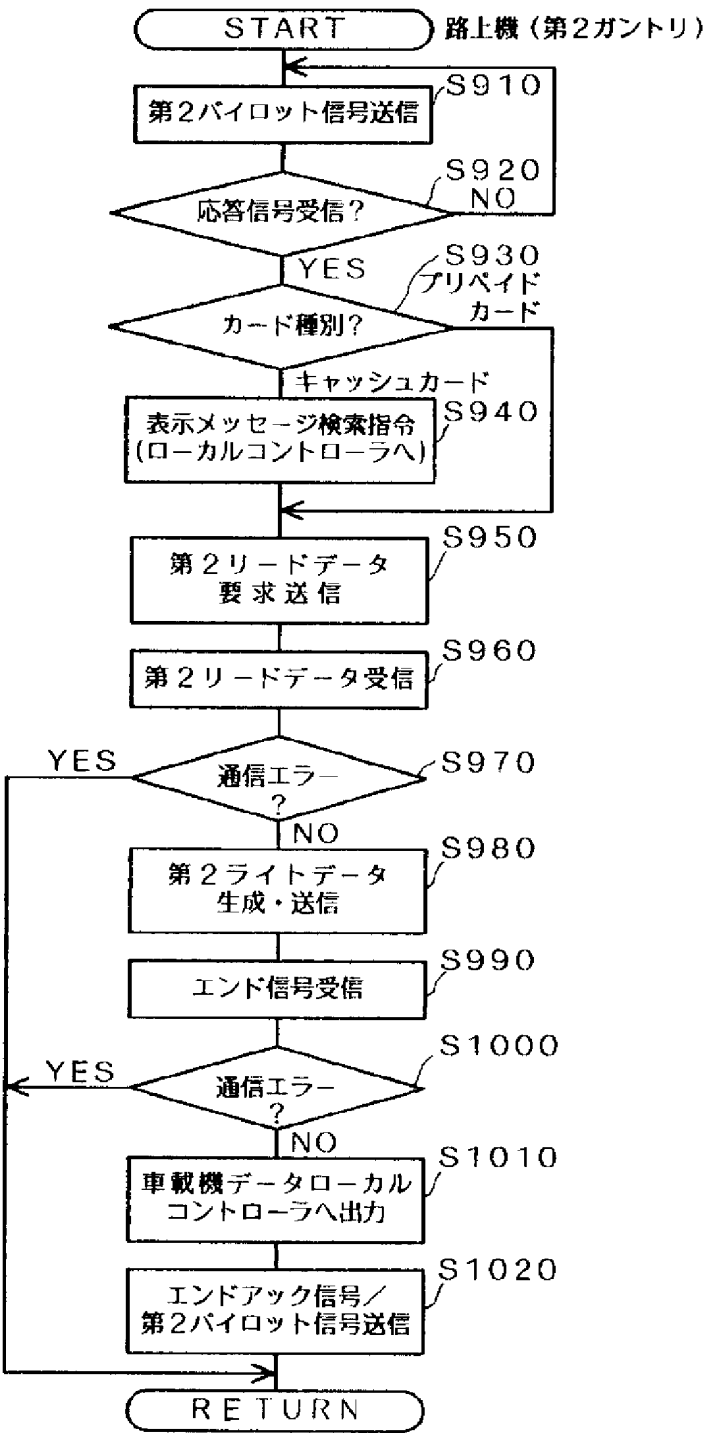
【図6】



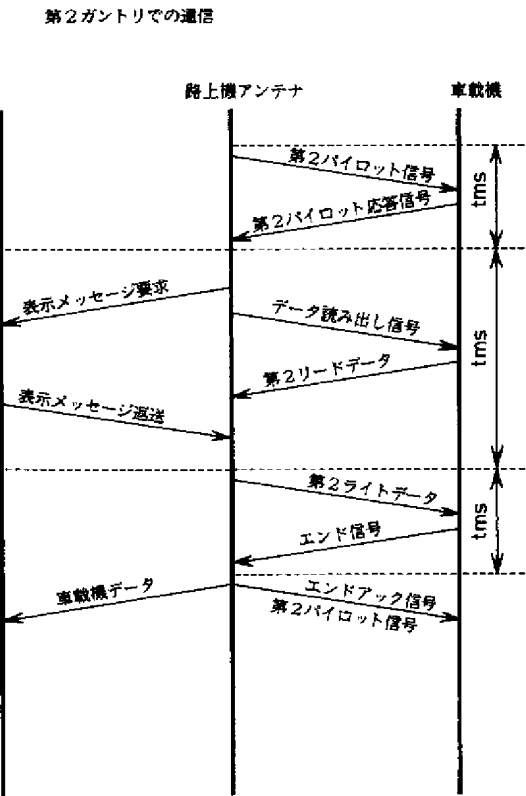
【図9】



【図10】



【図11】

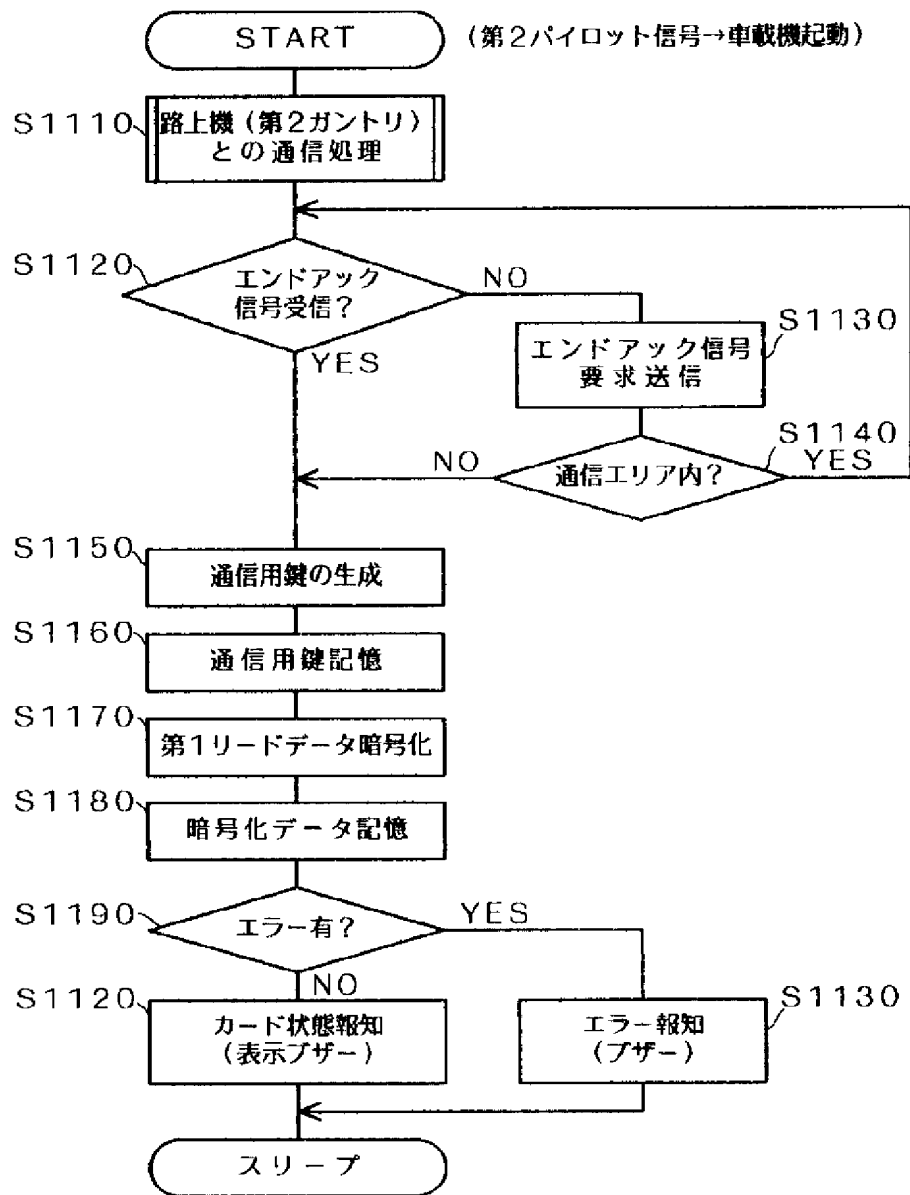


【図12】

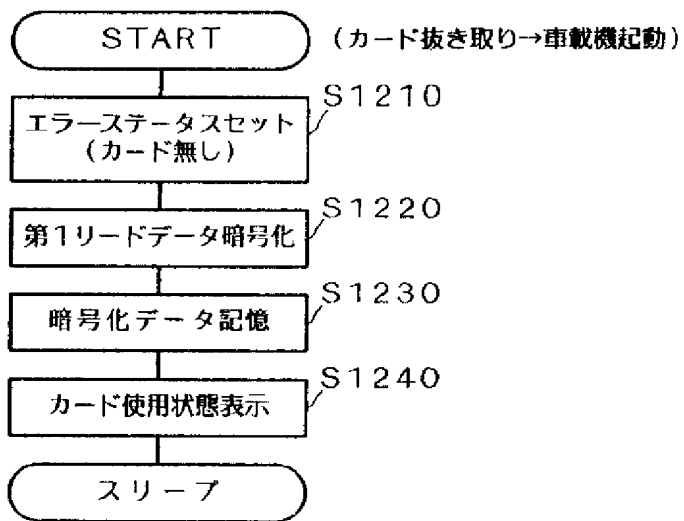
第2ガントリでの通信信号	内 容
第2パイロット信号 (路上機)	第2パイロット信号 場所番号
第2パイロット応答信号 (車載機)	応答コード 支払モードデータ
データ読み出し信号 (路上機)	データ読み出し命令
第2リードデータ (車載機)	応答コード ①キャッシュカード ファイル(一部を暗号化) ②ステータスコード ③支払方法 ④料金徴収結果 ⑤車載機コード ⑥CAN ⑦乱数 R3 ⑧料金徴収証明データ
第2ライトデータ (路上機)	書き命令 表示命令 表示メッセージ
エンド信号 (車載機)	応答コード
エンドアック信号 (路上機)	END ACK

① 車載機で暗号化

【図13】



【図14】



【図15】

入リロガントリ	
入リロガントリでの通信信号	内 容
入リロパイロット信号 (路上機)	パイロット信号 場所番号
入リロパイロット応答信号 (車載機)	応答コード 乱数 R1 暗号鍵番号 Kn
データ読み出し信号 (路上機)	データ読み出し命令
入リロリードデータ (車載機)	応答コード @ステータスコード @支払モード @車載機コード
入リロライトデータ (路上機)	書込命令 #車載機コード #場所番号 (一部を暗号化) トランザクションタイプ 入場 年 月 日 入場時刻
エンド番号 (車載機)	応答コード
エンドアック信号 (路上機)	END ACK

◎ 車載機で暗号化されるデータ # 路上機で暗号化されるデータ

【図16】

出口第1ガントリ

第1ガントリでの通信信号	内 容
第1パイロット信号 (路上機)	パイロット信号 場所番号
第1パイロット応答信号 (車載機)	応答コード 乱数 R1 暗号鍵番号 Kn
路上機認証メッセージ (路上機)	応答コード 乱数 R3 暗号鍵番号 Kc
入リロデータ (車載機)	応答コード @車載機コード @入リロ場所番号 @入場年月日 @入場時刻
データ読み出し信号 (路上機)	データ読み出し命令
第1リードデータ (車載機)	応答コード @ステータスコード @支払モード @車載機コード @CAN @残高 (途中まで暗号化) CSN XOR CAN CTC 使用する鍵のインデックス
第1ライトデータ (路上機)	書込命令 #車載機コード #料金総額 #場所番号 (途中まで暗号化) トランザクションタイプ 年月日 時刻 課金用データ (時間または出口番号)
エンド番号 (車載機)	応答コード
エンドアック信号 (路上機)	END ACK

◎ 車載機で暗号化されるデータ # 路上機で暗号化されるデータ